END-USER AWARENESS OF AND ADHERENCE TO CRISIS PREPAREDNESS OF THE INFORMATION SYSTEMS IN NEW ZEALAND ORGANISATIONS

By

DENNIS BUBERWA ISHUMI

A thesis submitted to the Victoria University of Wellington in fulfilment of the requirements for the degree of Master of Commerce in Information Systems

VICTORIA UNIVERSITY OF WELLINGTON

2013

Abstract

A crisis is a specific, unanticipated, and non-routine event that generates high levels of uncertainty and jeopardizes high value priorities such as life, economic well-being, or physical infrastructures. Some scholars observe that our computing environment has dramatically changed and is now defined by greater use and dependence on technology, while simultaneously it is hampered by technological failures and security vulnerability, which have perhaps led to an increase in the incidence of organisational crises. Because of the high occurrence of crises and the increased dependence on information systems (IS) in organisations, one would assume that most firms would have established measures to counteract these events, however the literature indicated otherwise. The purpose of this research was to explore and understand the factors that contribute to crisis preparedness of the information systems.

A comprehensive review of the literature indicated that the IS field has a large volume of publications on information systems disaster recovery, business continuity, information systems risk management and information systems security but little on crisis preparedness of the information systems. This study comprehensively reviewed relevant literature on the nature of crises, crisis preparedness and information systems. The literature review established groundwork necessary for the development of the research hypotheses which were tested during this investigation.

A quantitative positivist research approach was proposed. The study utilized a web-based survey to collect quantifiable information on the subject matter from study participants. The survey instrument was developed based on seven research dimensions. From these dimensions descriptive questions were created which formed part of the survey instrument. The collected data was analysed using three different approaches: descriptive statistics, correlation and percentage responses. From the data, facts about crisis preparedness of the information systems in New Zealand organisations were revealed.

In total 90 responses were received, 72 of which were eligible for data analyses. The study findings indicate some degree of end-user awareness of and adherence to crisis preparedness of the information systems in New Zealand organisations. However, more emphasis is needed in the understanding of the processes that bring about successful CPIS strategies across varying organisation structures.

The academic value of this research is the review of discourse in the fields of crisis preparedness and Information Systems, and the application of some of the theoretical concepts from those fields. These were necessary to test the research hypotheses and their findings can be used to explain the crisis-preparedness phenomenon in future studies. The practical value of this research is the development of a tool that can be used by managers and senior executives to undertake informed decisions with regard to the status or progress of the crisis preparedness of the information systems initiatives in their respective organisations from the end-user perspective.

Acknowledgements

My sincere gratitude and appreciation goes to my wife Marge, my daughter Bernice and my son Ellyson who allowed me to hide in the upper room to ensure that I brought this work to completion.

My sincere appreciation also goes to Dr. Philip Calvert, my supervisor who took the responsibility to guide me at every stage of the project. I would like to take note of his positive criticism on the text and some of the key concepts of this thesis and every contribution he made to bring this project to completion.

I would like thank my parents, Prof. A. G. Ishumi and Martha for being supportive throughout this process despite the physical distance. Dad, "I cherish your time spent on reading this thesis and your comments on some formatting issues". Unfortunately, my mother (Martha) could not see the finished project as she passed away when the project was underway.

I am thankful to our family friends Ian and Sandi Stevens for reviewing my grammatical errors and providing moral support throughout the project. This includes my colleague Jason Sutherland for acting as a bridge to approach some of the organisations that I needed to participate in this study.

My colleagues and students at the school of Information Management – Pak Yoong, Mary Tate, Dan Dorner, Marta Vos and others — for their encouragement and valuable support at different stages of this journey.

Finally, my thankfulness goes to practitioners in different sectors and organisations in New Zealand, particularly from the cities of Wellington and Auckland who supported this study.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AORN	Association of peri-Operative Registered Nurses
BCP	Business Continuity Plan
CIO	Chief Information Officer
CPIS	Crisis Preparedness of the Information Systems
FEMA	Federal Emergency Management Agency
FTC	Federal Trade Commission
HEC	Human Ethics Committee
IS	Information Systems
ISDRP	Information Systems Disaster Recovery Plan
IS/IT	Information Systems and Information Technology
IT	Information Technology
ISO/IEC	International Organization for Standardization (ISO) and International Electro-technical Commission
ISRM	Information Systems Risk Management
ISS	Information Systems Security
NASA	National Aeronautics and Space Administration
PMT	Protection Motivation Theory
SAA/SNZ HB	Australian and New Zealand Handbook
S.D	Standard Deviation
TRA	Theory of Reasoned Action
UN/ISDR	United Nations and International Strategy or Disaster Reduction
US	United States of America

Definitions

Availability:
This is an attribute to which information and associated assets are accessible by authorised users when required (Evans, 2003). In other words, it reflects the readiness for correct service (Avizienis, Laprie, Randell, & Landwehr, 2004).

***Business Continuity Plan*:**
This is a process of planning to generate a state of readiness that will facilitate an immediate response to a disaster affecting a business unit or the computing environment of an organisation (Smith & Jamieson, 2006).

Confidentiality:
This is a property that information is not made available or disclosed to unauthorised individuals, entities, or processes (Evans, 2003) or the absence of unauthorised disclosure of information (Avizienis et al., 2004).

Disaster Recovery Plan:
Documented procedures that establish how a company or organisation can restore its IS systems and services after a significant large-scale interruption (Omar, Alijani, & Mason, 2011).

Integrity:
This is a property of a computing environment that ensures accuracy and completeness of information and processing methods are safeguarded (Evans, 2003). In other words, it is the absence of improper system alterations (Avizienis et al., 2004).

Information Security:
Information security is a recurring management process in which risks are continuously managed by applying appropriate safeguards to reduce the likelihood and or mitigate the consequences of unacceptable risks (Albani, 2011). In other words, information security methods are intended to assist organisations to establish a security plan to address vulnerability associated with unauthorised misuse of information (Watson, 2007).

Information Systems Risk Management:
This is a management process which is intended to minimize the total expected cost of loss by selecting and implementing an optimal combination of security measures (Rainer, Snyder, & Houston, 1991). This process involves identifying, controlling, and mitigating information system–related risks (Elky, 2006).

Reliability:
This refers to the ability of the IS/IT asset to tolerate faults that may render it unusable or incorrect (Evans, 2003) or the continuity of correct service (Avizienis et al., 2004).

Threat:
A threat is any person, object or circumstance that has the potential for causing an IS failure (Watson, 2007).

Vulnerability:
Vulnerability is a property of an IS/IT asset that can lead to the compromise of one or more of its required attributes (e.g. confidentiality, integrity and availability) (Whitman & Mattord, 2005).

Botnet:
A botnet is a set of compromised computers, or bot clients, running malicious software that enables a "botherder" or "botmaster" to control these computers remotely (United States Computer Emergency Readiness Team, 2010).

Chapter 1: Introduction

The topic of the thesis is end-user awareness of and adherence to crisis-preparedness of the organisation's information systems (CPIS). To start this chapter, the concept of a crisis is explored to clarify the way it will be used in this thesis. Next, the motivation to undertake this study is explained in terms of a perceived gap in existing research. The research question(s) and the research objectives are then presented, followed by a discussion of the practical and academic value of this study. Having framed the topic and the motivation of the study, a brief description of the research methodology is provided. Finally, the structure of the main chapters in the thesis is presented.

1.1 The Concept of a Crisis

A crisis is a specific, unanticipated, and non-routine event that generates high levels of uncertainty and jeopardizes high value priorities such as life, economic well-being, or physical infrastructures (Denis, 1995). Crises manifest themselves in many forms such as informational (e.g. theft of proprietary information), physical (e.g. industrial accident), psychopathic (e.g. product tampering), or natural (e.g. earthquake) (Kim, Cha, & Kim, 2008; Mitroff, 2004). The frequency and diversity of types of crises have been on the increase (Pollard & Hotho, 2006) in the past three decades. Many Information Systems (IS) crisis events are associated with technological failures and security issues. Recently the rise of crisis events has become even more likely to a result of increased online criminal activities (Savage, 2002; Omar et al., 2011; Symantec, 2012).

Many of the crises incidents directly affect the IS because most of the operations and services provided by organisations are computerised and fully depend on the IS platforms to be effected. The importance to the organisation of having its information systems remain up and running is evident from the fact that critical business systems which run over the IS platforms are considered to be the backbone of the organisation (Chang & King, 2005). These authors also equate the information systems to the existence of the organisation itself. Moreover, crises happening today have become more complex given the interconnectivity nature of functional groups within and between organisations. As a result, in any given event a substantial number of processes, operations or activities running over the IS platforms are likely to be affected, both in the organisation and for external customers. This complexity has

led each crisis to last longer in comparison with previous years (Boin & Lagadec, 2000; Hart, Heyse, & Boin, 2001).

1.2 Motivation for the Research

The IS field has developed several ways to handle crises: managing disaster recovery, maintaining business continuity, IS risk management (ISRM), and IS security (ISS). Organisations need these processes in order: to prevent (Albani, 2011; Pinta, 2011), to minimize (Boin & Lagadec, 2000; Pinta, 2011), to control (Hough, 2005; Hu, Hart, & Cooke, 2006) or to recover (Nelson, 2006) from crises events. These approaches assist organisations to establish mechanisms to handle crises events before they happen, when they are in progress and after the events. Many studies on disaster recovery, business continuity and IS risk management have their main focus on what is perceived to be 'best practice' for these approaches at the organisation level. Even with this knowledge, the financial burden incurred by organisations due to the damages caused to the information systems has been on the rise (Richardson, 2007).

Critical business systems are essential to ensure that end-users within the organisation are able to carry out their daily duties, and managers will hope that a high level of work output from end-users guarantees optimal service delivery to the customer, for at the end of the day this generates revenue to the organisation. However, the same end-users are required to comply with a number of IS protection measures such as information security procedures and information security policies (Pahnila, Siponen, & Mahmood, 2007a). The processes by which end-users interact with the critical business systems and associated requirements to comply with established CPIS measures is critical because in many cases end-users are taken by surprise due to a lack of awareness of (Siponen, 2000), or a lack of involvement in the processes used to establish these measures (Savage, 2002).

The ever-rising cost of undoing the damage that results from IS crises events is an international problem, and clearly one that can and will affect many organisations in New Zealand. There is no clear evidence of past research studies on end-user awareness of and adherence to crisis preparedness of information systems in New Zealand organisations. These two conditions were the main drivers that led to the undertaking of this study. Therefore, this study aimed at investigating the degree to which end-users are aware of and adhere to CPIS measures in New Zealand organisations.

1.2.1 Research Gap and Research Question(s)

IS are essential to organisational success (Bharadwaj, 2000; Mithas, Ramasubbu, & Sambamurthy, 2011). These systems are used to integrate various business activities, to reorganize and enhance interactions with customers, and to coordinate organisations with their suppliers so that customer demands are dealt with more efficiently and effectively. To take advantage of a wide range of capabilities offered by the IS, many organisations have underpinned almost all activities, operations or processes over different IS platforms. End-users, also known as IS-users, use these platforms to process, to support, to operate, to develop, or to manage the information systems services and applications within and outside the organisation (Chang & King, 2005).

Despite the level of computerisation, organisations are still affected by crises events. Crises events are potentially capable of generating substantial negative impacts on the functioning of the organisation. Crises events in the context of the IS manifest themselves in diverse forms such as destruction of the organisational information base (Pearson & Clair, 1998), informational (theft of proprietary information), physical (industrial accident) (Kim, Cha, & Kim, 2008; Mitroff, 2004) or data loss (data corruption) (Omar et al., 2011).

In order to counteract these adverse events some organisations have committed to a crisis management process (CMP). CMP is a process that embraces four main stages: mitigation, preparedness, response and recovery (Shaluf, 2008). These are processes that organisations establish in order to prevent, minimize, and control the negative impact resulting from crises events. From these processes different measures are deployed in order to transcend the ramifications resulting from the impact of crises events. Some of these measures include business continuity plans (BCP), disaster recovery plans (DRP), ISS, and ISRM.

These measures, which are established during the mitigation phase, are meant to provide a sense of being ready to offset the effects of crises events in times of response and recovery. They are intended to have the organisation ready to react to complex situations once they are in progress. On the other hand, preparedness is a proactive process that plays a vital role to ensure that response and recovery phases are executed effectively given the crisis event (Boin & Lagadec, 2000; Eaglestone, Lin, Nunes, & Annansingh, 2003). The importance of crisis preparedness is made evident in organisational partnerships. This is because an organisation

that implements proactive approaches is considered as a trusted partner, which also reflects upon its high reputation in the eyes of other organisations (Allen, 2005). While crisis preparedness is vital for organisations in business partnerships, its significance is far more important at the organisation level. Albani (2011) notes, that "…information security policies and procedures are of little use unless they are understood and observed by all who are affected by them" (p. 96). This observation is referring to the necessary level of end-user involvement with CPIS within the organisation. Albani suggests that organisations should proactively communicate their expectations and requirements to their employees, because it is insufficient to publish policies and assume that end-users are aware of them, will read them and will adhere to them. In other words, organisations should proactively prepare IS-users to function moderately well even in crisis times and assist them to bring up threatening issues in their organisations on a day-to-day basis (Boin & Lagadec, 2000).

While the three components involved in the CMP (i.e. mitigation, response and recovery) are well explored in the literature there remains a huge concern on the fourth component—preparedness. The major challenge with crisis-preparedness is about the understanding of preparedness measures. The lack of understanding or awareness of what actually constitutes crisis-preparedness of information systems has a detrimental effect on how organisations prepare their employees (end-users) to participate in crisis preparedness endeavours (Siponen, 2000; Susanto, 2003). Consequently, this has led to confusion and ultimately to low levels of preparedness.

A study conducted by Meta Group research (2003) cited by Susanto (2003) reports that only 20% of Global 2000 organisations have comprehensive BCPs to assist them in recovery operations. The major problem that causes the lack of crisis preparedness is the failure to prioritize measures for crisis preparedness of the information systems. Adding to this problem is the inability of the managers to differentiate between different measures that are appropriate to establish the crisis preparedness of the information systems (Susanto, 2003). For example, some organisations consider a business continuity plan to be synonymous with a disaster recovery plan, yet in essence these two plans have different purposes.

The lack of crisis preparedness is more of an attitude problem (Jordan, 1999). This is because in many instances the responsibility for producing the so called "plans" (e.g. BCP, DRP) to assist in times of crisis events is usually given to a particular group of people (e.g. low level

personnel from the IS/IT department), hence no other staff are involved, and do not appreciate its importance (Cerullo & Cerullo, 2004). This may happen because the management perceive crisis preparedness to be irrelevant as far as information systems are concerned, and hence, they don't give it the attention it requires. The attitude problem is also reflected in issues related to risk and security policies. For instance, in some organisations more emphasis is placed on the technology and ignoring other components like end-users awareness and training, policies or IS standards operationalisation (Wood, 1995; Botha & Solms, 2004).

The set of scenarios highlighted above indicate that there is a problem and hence a research gap that needs to be addressed. Therefore in order to address this gap, this study investigates the following research question(s):

1. What constitutes crisis preparedness of the information systems?

2. What is the extent of end-user awareness of crisis preparedness of the information systems within the organisation?

3. What is the extent of end-user adherence to crisis preparedness of the information systems in the organisation?

1.2.2 Research Objectives

Much of the reviewed literature relevant for this study indicated that failure to counteract crisis events in organisations was in part inherent in end-user understanding, end-user awareness of, and end-user failure to abide by established CPIS measures. What was inferred from these studies is the deficiency in aligning the crisis preparedness initiatives to a human (end-user) component. On the basis of this understanding, the main theme for this research was to identify and compile the key elements of the CPIS from the extant literature. This undertaking established a foundation to generate research items which would later be used to seek opinions from end-users in their actual work settings. This involved identifying the extent to which end-users were aware of different aspects of CPIS and to what degree they were actually ready to act on different measures of CPIS established within the organisation. Thus, this research had four main objectives.

1. To determine the key elements of the CPIS;
2. To determine the extent of end-user awareness of CPIS measures in their organisations;
3. To determine the extent of end-user adherence to CPIS measures established within the organisation;
4. To apply two existing theories to test the research hypotheses on end-user awareness of and adherence to CPIS measures in New Zealand organisations.

1.3 Value of This Research

The primary value of this research to academia is the expansion of the existing discourse on crisis-preparedness. This was done through the application of two existing theories to create research hypotheses and test them. Both, the Theory of Reasoned Action (TRA) and the Protection Motivation Theory (PMT) are important in the study of uncertainty or adverse events. While the PMT is useful in investigating the cognitive processes mediating behavioural change, the TRA is vital in the prediction of end-user intentions and end-users' behavioural change attempts. The consolidation of the theoretical frameworks and the application of the theories to analyse data and test the research hypotheses add knowledge to the field of crisis preparedness in IS.

This study also offers value to the practitioners. The significance of the results from this study allows the practitioners to gain a better understanding of the level of end-user awareness of and adherence to crisis preparedness of the information systems in their organisations. From this understanding organisations are able to improve or enhance user participation in crisis preparedness of the information systems initiatives at all levels.

1.4 Research Methodology

In order to address the research questions and the main objectives of this research it was important to review the relevant literature. This was fundamental to gain a deeper understanding of the extant literature in the subject matter. Moreover, the review of the literature permitted for the identification of the theoretical foundations on which to base this study.

The classification of the theoretical foundations to support this study allowed for identification of the research dimensions. The research dimensions permitted the generation of the research hypotheses and the creation of research items/statements for the survey instrument.

A quantitative positivist research approach was adopted. The aim of this methodology was to collect quantitative data that could explain the CPIS phenomenon without requiring subjective interpretation. The data was collected by using a web-based questionnaire. The data was analysed using three different methods (descriptive statistics, correlation and percentage responses) in order to provide facts about end-user awareness of and adherence to CPIS measures in New Zealand organisations.

1.5 Thesis Outline

This chapter presents the introduction of the thesis. Chapter 2 presents the literature review by addressing the three main areas of this study, namely the nature of a crisis, crisis preparedness, and information systems. This chapter provides a thorough review of the theoretical concepts relevant to the investigation. Chapter 3 explains the research methodology that guided this investigation. Chapter 4 analyses the collected data and presents the findings. Finally, Chapter 5 provides an overview of the study, presents the study implications and study limitations. The chapter closes by presenting opportunities for future research.

Chapter 2: Literature Review

2.1 Chapter Outline

This chapter reviews and discusses the literature relevant to this study. The review considers a number of research streams in order to understand the literature on the subject. Most of these works are from business continuity planning, information systems risk management, information systems disaster recovery planning, and information systems security.

This study builds on the common tradition of IS research of drawing on theories from disciplines such as economics, computer science, psychology and general management (Wade & Hulland, 2004). It is envisaged that theories and/or concepts from relevant disciplines will shed more light on understanding and investigating crises preparedness in the information systems (IS) context.

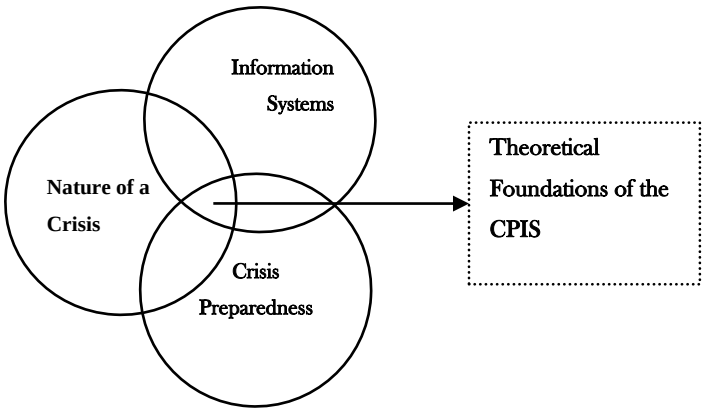

Figure 2.1: Literature Review Structure

The literature review is divided in three main sections: 1) the nature of a crisis; 2) crisis preparedness and; 3) information systems. Figure 2.1 is a diagrammatic representation of the extent of this literature review. This diagram is used as a guide to review systematically appropriate literature in relation to the three main research areas.

From section 2.1.1 to section 2.1.5 the review explores the general understanding of crises in the current literature with respect to this study. From these sections, the reader is able to see the general perspective of crises in the context of information systems within organisations

but with a particular focus on New Zealand organisations. The crisis object is defined, followed by the characterisation of the conditions that trigger crises in a computing environment. This section is completed with a discussion of various issues associated with crisis management process in current practices.

Section 2.2 reviews and discusses the concepts of crisis preparedness. In this section the concept of crisis preparedness is defined in order to provide a lead to section 2.3, the Information Systems.

Section 2.3 reviews the significance of the information systems and hence the importance of being crisis ready from the end-user perspective. Section 2.4 reviews the foundation concepts in order to identify the theoretical framework to guide this investigation.

2.1.1 Overview of Crises

The concept of crisis is inherent in many aspects of IS such as security, interdependencies that result from a highly inter-connected world, human error and climatic disturbances (Robert & Lajtha, 2002). As a result, there is no agreed definition of a crisis. Given the lack of consensus on the common definition of a crisis (Shaluf, Ahmadun & Said, 2003), scholars from different disciplines use the terms "crisis and disaster[1]" interchangeably or meaning the same thing (Brown, Hickling, & Frahm, 2010; Faulkner, 2001; Racherla & Hu, 2009; Sylves, 2008). The use of the term 'crisis' is very much dependent on the scholar's area of research and the context in which it is being used (Preble, 1997). Building upon this understanding, this study explores the concept of crisis preparedness from the IS context. Therefore, this thesis draws on the work of Denis (1995) and defines a crisis as "a specific, unanticipated and non-routine event that generates high levels of uncertainty and jeopardises high value priorities such as life, economic well-being, or physical infrastructures including availability, confidentiality, integrity and reliability of information systems within the organisation".

In the past three decades the world has witnessed a considerable number of adverse events which led to the damage of IS platforms (Hu et al., 2006). The losses have been experienced

[1] In this study the terms: crisis, disaster, emergency and catastrophic or adverse events are considered to mean the same thing and may be used interchangeably.

by a wide range of industries. For instance, in 1990, AT&T's nationwide network went down due to a software failure (Kuhn, 1997). Likewise, Sun Microsystems Inc. registered reduced net income for the fourth quarter due to system errors which affected the introduction of a new company-wide computer system (Rainer, Snyder, & Carr, 1991).

In 1989, the American Airline's Sabre computer reservation system inadvertently shut down for almost 12 hours (Rainer et al., 1991), and the event disrupted the operations of about 14,000 travel agencies nationwide. This was because a substantial amount of customers' information (data) related to flight bookings was wiped from the airline application system. One study reported losses resulting from these kinds of events to the tune of US$345,000 on average among the 39% of organisations approached during the time of the study (D'Arcy, Hovav, & Galletta, 2009). Unfortunately, 50%–75% of these events are triggered from within the organisations (Ernst & Young, 2003).

Sometimes crises happen as a consequence of human actions. These actions involve personnel within the organisation who deliberately perform acts of vandalism, theft (Whitman & Mattord, 2005) or non compliance with established rules and regulations (Jones, 2007). For example, IS personnel responsible for the management of customer information such as credit card details may sell that information to a third party, which can also lead to identity theft. The illegitimate sale of customer information is a threat both to the organisation and to those outside of the organisation. Identity theft can negatively affect the brand and reputation of the organisation, which also can result in a loss of investor and consumer confidence and loyalty (Allen, 2005).

The seriousness of these actions to the organisation is clearly demonstrated by the incident that involved a U.S credit information provider back in 2006. This provider, ChoicePoint Inc., was fined US$10 million for negligence after personal information of 160,000 people went missing (Herrmann, 2007). The failure by ChoicePoint to protect private data from the threat of identity theft (FTC, 2006) had rendered it financially liable in terms of insurance payments and restoring its reputation in that market segment (or to its stakeholders).

The preceding four paragraphs demonstrate how crises can have a direct impact on the IS platforms and the whole computing environment of an organisation. The identified examples

highlight some types of crises that are potentially capable of causing large detrimental impact to the IS. According to Pearson and Clair (1998), some other types of crises events include:

- Natural disasters that destroy the infrastructure that supports a certain product or service;
- Natural disasters that destroy the organisational information base;
- Information systems tampering— an informational event that leads to criminal activity or unauthorised system access;
- Information sabotage that develops into a negative financial impact as a result of fraud activities or disruption of business operations;
- Security breaches that takes down the enterprise network.

The consequential impact resulting from these events is enormous (Cerullo & Cerullo, 2004). Unfortunately, the frequency of these events and others of a similar nature is increasing and they are becoming more serious day by day (Jain & Singh, 2012). For instance, the number of attacks to the organisational IS from the Internet has increased from 3.0 Billion in 2010 to 5.5 Billion attacks in 2011 (Symantec, 2012). Despite the current investments in management methodologies and technologies such as information systems risk management, information security risks, business continuity plans, and disaster recovery plans to assist managers in addressing challenges resulting from adverse events (Jordan, 1999; Susanto, 2003; Sam, 2004; Omar et al., 2011), problems remain for which end-users are often unprepared (Spillan & Hough, 2003). These problems are further complicated by the lack of understanding and/or awareness of the fundamental concepts of crisis preparedness, or how to be prepared given the wide range of potential crises that can affect the functionality of the IS platforms.

2.1.2 Types of Crises in the Context of IS

Crises events are classified differently depending on the condition in which they occur. The UN International Strategy for Disaster Reduction suggests two main types of crisis events: natural and technological (UN/ISDR, 2002).

Natural crises include two explicit groups, namely:

1. Hydro-meteorological crises.

These include floods and wave surges, storms, droughts and related calamities such as extreme temperatures and forest/scrub fires, and landslides.

2. Geophysical crises.
   These are categorized into earthquakes, tsunamis and volcanic eruptions.

Technological crises are mostly associated with industrial accidents. These are incidents such as chemical spills; collapses of industrial infrastructures; explosions; fires; gas leaks; poisoning; and radiation.

Both hydro-meteorological crises and geophysical crises are potentially capable of disrupting the IS platforms within the organisation (Cerullo & Cerullo, 2004; Omar et al., 2011). The disruption could result from flooded data centres due to storms or physical destruction of the IS infrastructure due to earthquakes. The IS platform could also be damaged due to technological crises from industrial accidents such as fires and explosions (Omar et al., 2011). While some technological types of crises might be rare such as fires and explosions, others are more common in the IS environment including power failure (Elky, 2006), communication line failure, and defective equipment (Jordan, 1999; Cerullo & Cerullo, 2004) as well as malicious threats (e.g. viruses and worms) from inside and outside the organisation (D'Arcy et al., 2009).

Technological crises are also evident from the occurrence of cyber-terrorism— unauthorised access to a system, denial-of-service attack, or unauthorised use of a system (Cerullo & Cerullo, 2004). The likelihood of different IS platforms shutting down due to unauthorised access to a system, denial-of-service, unauthorised use of a system, or unauthorised changes to system hardware or software is on the rise. In part, this is because many organisations have increased their dependence on IS to facilitate their day to day operations as well as linking internal to external networks (Savage, 2002; Omar et al., 2011), and as such, IS platforms are more prone to security vulnerabilities and technological failures. These characteristics make the IS platforms a potential target for all sorts of attacks— for example malicious attacks and cyber-terrorism. The extent of damage from technological crisis events is similar to those generated from natural crises (Cerullo & Cerullo, 2004).

Having explored different forms of crises and their impact on the IS platforms in the organisation, the next section explores the conditions that trigger different types of crises.

2.1.3 Conditions that Trigger Crises in an IS Environment

The categorization of crises in natural and technological types (UN/ISDR, 2002) seems to be insufficient. This is because crises events are likely to result from other causes beyond natural and technology. For instance, the IS environment encompasses a wide range of other components such as individuals, organisations, or systems that collect, process, or disseminate information. Any of these components is a likely candidate that can initiate a sequence of events that can lead to a crisis. To allow for this, the concept presented by UN/ISDR (2002) is further developed to reflect triggers of crises in an IS environment. They include human (e.g. perceptions, behaviours), organisational (e.g. management miscommunication, management carelessness or management misconduct), technological (e.g. accidents, defective equipment, systems changes and new technology) and natural (e.g. floods, earthquake or storms). Table 2.1 summarizes the four key triggers of crises in an IS environment.

Table 2.1: Key Triggers of Crisis Events

Category	Triggers	Author
Human	Perceptions, behaviours, poor training, lack of motivation, evil intent, poor decision-making, lack of knowledge, operator error, managerial errors, human error	Rousaki and Alcott (2006); Weirich and Sasse (2001) ; Rhee & Kim (2005); Garrett (2004); Parnell, Koseoglu, and Spillan (2010)
Organisational	Management miscommunication, management carelessness, takeovers and mergers, layoffs, management misconduct, policy failures, inadequate resource allocations	Rosenthal and Kouzmin (1997); Shrivastava, Mitroff, Miller, and Miclani (1988); Jaques (2010)
Technological	Accidents, defective equipment, systems changes, adoption of new technologies, cyber-terrorism activities, malicious threats	Perrow (1999); Cerullo and Cerullo (2004); Shaluf (2008); D'Arcy et al., (2009)
Natural	Floods, storms, earthquake	Coleman (2006); Jaques (2010); Shrivastava et al., (1988)

Human

There are different elements in human nature that are potentially capable of initiating crises. They include perceptions (Rousaki & Alcott, 2006), behaviours (Rhee & Kim, 2005) and poor training (Garrett, 2004) among others . The perception aspect is well described by

Chinese and Greek wisdom that characterises a crisis as having two sides: positive and negative. From this perspective the concept of a crisis is symbolised by combining the signs of danger and opportunity (Robert & Lajtha, 2002; Rousaki & Alcott, 2006). The ability to differentiate a danger from an opportunity, and vice versa, from a crisis event depends very much on the individual's perception, on how the individual was brought up, or the previous experience with the incident at hand (Parnell, Koseoglu, & Spillan, 2010). In other words, differences in perceptions allow individuals to act differently when faced by new events or complex situations. Depending on which action is taken may result in a crisis event or the avoidance of it.

The human element in crisis events can further be illustrated by the use of secure passwords to access various IS resources (*Assuming the use of secure passwords as one aspect of the CPIS*). It is known from the literature that system users behave differently when it comes to the use security measures. Inherent in their behaviour, some users may not feel they are vulnerable to relevant password security threats (Weirich & Sasse, 2001). Rhee and Kim (2005) also contend that because of security behaviours some computer users consider themselves less vulnerable to threats than their counterparts. Issues related to non-compliant behaviours of humans do not end with security passwords alone, but they are also evident in back-up procedures for end-user systems (Nelson, 2006), including organisational IS rules, routines and standards and virus checks (Jensen, Kjærgaard, & Svejvig, 2009).

Other potential triggers of crises in the human category are characterised as human factors. Because of the human factors, crises may occur as a result of actions or inactions of end-users or individuals in that particular organisation. The causes of such incidents are attributed to the human factors which include (a) a lack of knowledge and poor training, (b) unsafe behaviour, (c) leaning to poor decision making regardless of being aware and motivated and, (d) being motivated to act maliciously (Garrett, 2004).

Organisational

Triggers of crises under the organisational category include miscommunication, carelessness, and misconduct. Crises may occur as a result of simultaneous interactions among variables which co-exist inside the organisation with those in its environment (Parnell et al., 2010; Shrivastava et al., 1988). Usually, environmental variables introduce preconditions for triggering adverse events. The most recorded form of interaction in which failures occur is

miscommunication in decision making among the stakeholders (Elsubbaugh et al., 2004; Rosenthal & Kouzmin, 1997; Shrivastava et al., 1988). These types of failures build up in stages (Turner, 1976) through communication breakdown either at the departmental level or at the organisation level. The extent of communication failures are depicted in some of the major disastrous events like NASA's Challenger explosion, the Three Mile Island nuclear accident (Shrivastava, 1994), and the explosion of the Union Carbide Corporation pesticide plant in Bhopal, India, in 1984 (Roberts, 1990; Shrivastava et al., 1988; Shrivastava, 1994). Excessive optimism and system pressures were blamed as being the cause of the Challenger disaster (Starbuck & Milliken, 1988) because even though the concerned parties were aware of the potential technical flaws in the Challenger design they failed to communicate that information to the relevant bodies that could have prohibited liftoff.

Management carelessness or failure is also regarded as a key trigger of crises in the IS environment. Despite the organisation being bound to meet a range of societal legislative requirements such as information security incident management system standards (ISO/IEC 27035:2011), crisis management – guidance and good practice (PAS 200:2011), business continuity management (SAA/SNZ HB 221:2004), trade sector standards, and also best-practice standards and policies that have been adopted within the organisation field (Jones, 2007; Albani, 2011), some managers fail to establish proper procedures and structures to accommodate these standards. For instance, the management might be working against (i.e. show a lack of interest in) the laid down procedures and structures, resulting in limiting signal detection methods, inhibiting upward reporting and discouraging positive thoughts from key stakeholders (e.g. end-users) (Jaques, 2010).

From a different perspective, some of the failures mentioned above originate from organisational factors. This is according to Elliott and Smith (2006), whose standpoint was built on earlier arguments made by influential scholars such as Turner (1976) and Turner & Pidgeon (1997). Organisational factors include "policy failures, inadequate resource allocations for safety, strategic pressures which allow managers to overlook hazardous practices and conditions, communication failures, misperceptions of the extent and nature of hazards, inadequate emergency plans, and cost pressures which curtail safety" (Shrivastava et al., 1988, p. 290). The potential for a crisis event is nurtured through faulty assumptions in the organisation because organisational beliefs and cultures are incorporated into day to day management and its operations (Turner, 1976). Included in this category are the crises

resulting from takeovers and mergers, layoffs, management misconduct (Jaques, 2010), lack of organisational planning, and unwillingness to use appropriate resources to address a crisis in the making (Parnell et al., 2010).

Technological

Crises resulting from technical aspects originate from or through handling or operating of equipment as well as problems with the equipment itself. A small defect in the equipment is likely to escalate to a major crisis (Pearson & Mitroff, 1993). Technological crises resulting from accidents in different systems express themselves in multiple, simultaneous, and interacting failures in design, equipment, procedure, and environment (Perrow, 1999). A vivid example of these kinds of crises is the events that led to the plant explosion in Bhopal in 1984 (Shaluf, 2008). The plant exploded because it had received inadequate maintenance and was in a rundown condition (Shrivastava et al., 1988). The explosion was the effect of the interaction between material things (e.g. technologies), people and institutions. To explain this interaction Jasanoff (1993) notes that "a factory design that had worked more or less safely in America had been transported to a country with a fundamentally different material and technological culture" (p.128). As a result, the operators had developed their own way of running the plant in accordance with their own cultural necessities and assumptions.

The investigation of the accident indicated that constant malfunctions in valve and alarm systems had forced the workers to develop their own ways of dealing with the breakdowns. This included relying on their sense of smell as a detection system for the leaking of methyl isocyanate. The absence of clear procedures and regulations for operating the plant resulted in the operator's failure to perform critical procedures shortly before the accident took place (Shrivastava, 1994) and hence the incident developed into a crisis event.

Natural

Natural events that are potentially capable of triggering crises that can impact IS platforms and render them unreliable include floods, earthquake and hurricanes (Cerullo & Cerullo, 2004) among others. The impacts resulting from these events manifest themselves in diverse forms, such as crippling the IT infrastructure, flooding the data centres or causing power outage (Omar et al., 2011). The federal emergency management agency (FEMA) reports that between 1976 and 2001 a total of 906 major crises were declared in the US alone (Cerullo &

Cerullo, 2004) and the frequency and magnitude of major crises is increasing. To emphasize the severity of these events Schut (1990), as cited by Cerullo and Cerullo, contend that 43% of organisations hit by severe crises never reopen, and that another 29% fail within two years.

2.1.4 Common IS Risks and Threats in NZ Organisations

Besides losses from natural causes, such as earthquakes, fires and floods, the majority of adverse events to the information systems of the organisation can be traced back to either intentional or unintentional unsafe behaviour of end-users or individuals. The New Zealand Computer Crime and Security Survey showed that over 70% of participating organisations experienced some sort of security incident in the 2009 calendar year (Quinn, 2010). Many of these security incidents are directly linked to human actions or human behaviours. The survey involved respondents from utility, manufacturing /production, financial, telecommunications, transport, high technology, medical, wholesale, retail, tertiary education, legal, national and local government agencies, entertainment/media, construction, and commercial/trade services. Some of the incident types that are likely to generate negative consequences to the information systems of the organisation include *laptop/mobile hardware theft, virus contamination, malware infection, unauthorised insider access, unauthorised external access,* and *USB contamination*. Some types of incidents were not addressed during the 2010 survey, but seem to be significant in relation to IS risks and threats internationally. According to the recent Symantec Internet Security Threat Report (2012), these other incident types include *threats against mobile devices, spam* and *social media threats*.

2.1.4.1 Laptop/Mobile Hardware Theft

Theft or loss of a laptop, a computer or other medium on which data is stored or transmitted, such as a USB drive or a back-up gadget is considered to be the most common cause of data violation (Quinn, 2010; Tetmeyer & Saiedian, 2010). According to Quinn these losses cost the surveyed organisations NZ$250,000 during the 2009 calendar year. Across the globe laptops and mobile hardware theft account for 34.3% of all security breaches to the IS within the organisations. This equates to approximately 18.5 million identities being exposed to online criminals in 2011 (Symantec, 2012). The two reports indicate that the factors contributing the most to these losses are; (1) organisations being unaware that their mobile devices suffered security incidents and (2) a lack of security tools or procedures to safeguard

these devices that are fast joining the enterprise network (i.e. they appear to be preferred by employees to traditional desktop computers) (Albani, 2011).

2.1.4.2 Virus Contamination

A virus is defined as a small computer programme that reproduces itself on an infected computer and multiplies like a disease from one computer to another through e-mail, USB drives, file-sharing networks and Web sites (Goldsborough, 2007; Siponen & Oinas-Kukkonen, 2007). Viruses are second in importance to laptop/mobile hardware theft, costing about NZ$0.25m to participating organisations at the time of Quinn's study (2010).Virus attacks manifest themselves in a wide range of destructive incidents. These include loss of data, data inconsistency, or data corruption (Goldsborough, 2007). One recorded incident of a viral attack is the SQL Slammer (a worm) that hit Microsoft SQL Servers in the early hours of January 25, 2003. This worm took advantage of a bug found in the SQL Server that had been made public several months earlier (Aytes & Conolly, 2003). Despite this vulnerability being known to IS staff from many organisations they failed to apply a required patch to their respective systems until after the worm event. According to the report released by Symantec (2012), future attacks can be avoided if organisations and all involved stakeholders update security virus and intrusion prevention definitions on regular basis. This also includes conducting training and awareness programmes to key stakeholders in the organisation— the end-users (Siponen, 2000).

2.1.4.3 Malware Infection

“Malware” is a portmanteau word from ***mal***icious soft***ware*** (Australian Communications & Media Authority, 2008). Malware infection allows someone with an evil intent to gain full access to the compromised host, leading to the exfiltration of sensitive information or the installation of utilities that facilitate remote control of the host (Provos, McNamee, Mavrommatis, Wang, & Modadugu, 2007). Malware exists in diverse forms such as Trojan, Adware and Spyware (Australian Communications & Media Authority, 2008). Trojan software contains or installs a malicious programme with a harmful impact on a host computer. Adware automatically displays advertising material to the user resulting in a nuisance user experience. Spyware is malicious software secretly installed on host computers that collects information about users without their knowledge. Spyware software operates by monitoring the user's computing experience. Spyware can collect almost any type of data,

including user information like user logins, bank or credit account information, and Internet browsing habits (Sipior & Ward, 2008).

Quinn (2010), reports that malware infection is the third largest IS threat, experienced by 22% of the respondent organisations. This percentage is consistent with data published by Symantec (2012), which indicates that between October 2010 and the end of the year 2011 about 35.8% of organisational websites had at least one vulnerability and 25.3% had at least one critical vulnerability resulting from malware infection. In part this is encouraged by the integration of IS to the Internet which facilitates a number of business processes to be conducted online. As such computer users have become the target of an underground economy that infects hosts with malware or adware for financial gain (Provos et al., 2007).

Malware infections have become more common and trickier to detect and remove, as their perpetrators make use of many existing sophisticated techniques. For instance, Conficker had nothing new but was difficult to discover and erase because it was created by combining many advanced malware techniques (Markoff, 2009; Porras, 2009) . On the other hand, web-based malware infection is made possible to a large extent by the existing facilities to setup and deploy websites (Provos et al., 2007). Provos et al., observe that keeping the required software (IS platforms) up to date with patches is a challenging task since it requires human intervention that involves human behaviour with regard to crisis preparedness measures of the information systems.

2.1.4.4 Unauthorised Insider Access

One of the complicating aspects with improper insider access is that the referred incidents will not always relate to something that is unauthorised (Magklaras & Furnell, 2001; Furnell & Phyo, 2007). This is because the individual concerned has legitimate access to IS resources of the target organisation. In other words, this person does not need to bypass the access control mechanisms of the IS infrastructure for example by stealing passwords. In the context of this study, unauthorised insider access is the act of abusing granted privileges to cause harm (Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005), thus violating the established measures for the crisis preparedness of the information systems of the organisation.

Abuses of the information systems of the organisation are acts performed for a variety of reasons. For instance, a legitimate end user who attempts to access sensitive data (i.e. data

theft), take revenge against an organisation (personal differences) due to his/her impending redundancy, other malicious motives, or deliberately ignoring established measures for the crisis preparedness of the information systems (i.e. being negligent) (Furnell & Phyo, 2007; Richardson, 2008).

According to D'Arcy et al., (2009) unauthorised insider access of information systems resources represents a significant threat to organisations. This point of view is consistent with the finding from the New Zealand Computer Crime and Security Survey (2010) that reports that security policy non-compliance and inadequate protection from internal users are the second and third largest perceived issues, backing up the 2007 findings that the insider threat poses the greatest risk to organisational security.

Insiders are very often the source of major and costly security incidents, and a considerable proportion of what is commonly categorised as online crime (or cybercrime) can be attributed to them. Undeniably, their place within the organisation often puts them in an ideal position to access a system illegitimately if they are inclined to do so (Theoharidou et al., 2005; Furnell & Phyo, 2007).

2.1.4.5 Unauthorised External Access — Denial of Service Attacks

Denial of service (DOS) attacks have recently become a weapon to promote political ideology such as promoting expressive politics, free speech, and human rights by a number of social groups like Anonymous. A DOS attack is an attempt to make a machine or network resource unavailable to its intended users (Computer Emergency Response Team, 2001). The DOS attack is implemented by clogging up the memory of the targeted system so that it cannot be accessed by its users, or it causes the target system to crash, reboot, or otherwise deny services to legitimate users (Kumar & Gomez, 2010; Jain & Singh, 2012). The architects of DOS attacks usually target sites or services hosted on high-profile Web servers such as government websites, credit card payment gateways, and banks (see some examples below).

Internal Affairs website down; no evidence of DOS attack so far
February 2011

The Internal Affairs Department website is down, and while there has been speculation it may be due to a denial-of-service attack from the hacker group Anonymous, Internal Affairs spokesman Tony Wallace says there is no evidence so far to suggest that's the case.

Source: http://computerworld.co.nz/news.nsf/news/internal-affairs-website-down-anonymous-blamed

Walmart, Amazon.com hit with denial of service attack
Thursday, December 24, 2009

Holiday shoppers who were hoping to purchase last minute gifts at some of the top e-commerce retailers in the country were greeted with a surprise Wednesday evening as a denial of service attack slowed down sites such as Amazon.com, Walmart.com, Expedia and others.

Source:
http://www.bizjournals.com/seattle/blog/techflash/2009/12/walmart_amazoncom_hit_with_denial_of_service_atack.html

According to the US Computer Emergency Response Team (2001), not all service outages, even those that result from malicious activity, are necessarily denial-of-service attacks. Other types of attack may include a denial of service as a component, but the denial of service may be part of a larger attack. The authors further contend that illegitimate use of resources may also result in a denial of service. This happens when an unauthorised user uses the organisation's anonymous ftp area[2] as a place to store illegal copies of commercial software, which results in consuming disk space and generating network traffic.

Denial of Service attacks will have a greater impact as more services and business processes are moved over to the Internet platform. According to the New Zealand Computer Crime and Security Survey (2010) external threats (virus/malware/worms…) account for 46% of all IS threats and risks. DOS attacks can cause loss of business and credibility. However this can be avoided if the following vulnerabilities in the organisation IS platforms are sorted out (Evans, 2003; Albani, 2011):

[2] Anonymous ftp area is method for downloading public files using the File Transfer Protocol (FTP). It is called anonymous because the person downloading the files can not be identified.

- ✓ Apply an appropriate firewall to the IS infrastructure;
- ✓ Provide adequate network management;
- ✓ Apply patches to different versions of the software used in developing various IS applications that can stop the exploitation of any security weakness;
- ✓ Keep up to date all measures for the crisis preparedness of the information systems to allow known weaknesses to be corrected in a timely manner. This includes running training and awareness programmes to key stakeholders.

2.1.4.6 USB Devices

In the past decade Universal Serial Bus (USB) devices became commonly used as new forms of portable storage media with great storage capacities, high data transfer speeds, and are typically removable and rewritable (Rich, 2007; Tetmeyer & Saiedian, 2010). These kinds of devices include memory cards (Compact- Flash, Secure Digital or Memory Stick), removable USB flash drives, and iPods among others. The USB devices may also be referred to as transient storage devices (TSDs).

The small physical size of the USB coupled with functionalities such as the ability to store and auto-run applications straight from the devices has allowed for criminal acts like identity theft, data breaches and electronic fraud to be carried out easily by insiders (Al-Zarouni, 2006; Vijayan, 2006). Given this possibility USB devices have become a major IS threat and risk factor to organisations (Quinn, 2010; Tetmeyer & Saiedian, 2010). However, Yee (2004) suggests that, for a device to be effective and easy to use there should be a trade off between security and usability. "This underlying principle is applicable to security issues for transient storage devices. If devices are solely focused on security, usability will suffer." (Tetmeyer & Saiedian, 2010, p. 46)

The extent of the IS threats and risks from USB devices is made clear in the New Zealand Computer Crime and Security survey (2010) showing that USB devices are the main vectors for virus and malware infection, including being among the main vectors for data loss incidents. Some of the common incidents causing these states of affairs include: USB via 3rd party network segment, USB via antivirus laptop, USB PowerPoint by overseas visitor, USB by security guard and loss or theft of a USB device. The survey also indicates that over 50%

of respondent organisations had no existing protection against USB incidents. Around 17% completely disabled USB capability and only 6% had file copy protection.

The literature indicates that USB based attacks are closely linked to human factors in relation to IS security or crisis preparedness of the information systems for this matter (Al-Zarouni, 2006). Clear understanding of the human factors involved may establish potential IS threats and risks TSDs pose to organisations. As such raising awareness and training of IS-users about these threats may play a big role in reducing USB based attacks.

2.1.4.7 Threats against Mobile Devices

The number of employees bringing their own mobile devices such as smart-phones, tablets or laptops to work is on the rise (Symantec, 2012). While threats against mobile devices were not explored in the New Zealand Computer Crime and Security Survey (2010), the global trends to 'bring your own device' presents a major challenge to the crisis preparedness of information systems in many organisations. This is because of the difficulty in monitoring and controlling every device brought to the enterprise network. The risk here is that a device owned by an employee could have been or might be used for non-work activity that can potentially expose it to malware infections.

Many of the mobile devices can be used in the same way as desktop computers. The complex design and enhanced functionality of these devices present additional vulnerabilities as their security can be compromised when accessing public internet hot spots or home networks. These vulnerabilities, put together with the growing market share, make mobile technology an attractive, viable, and rewarding target for those interested in exploiting it (United States Computer Emergency Readiness Team, 2010). This is because mobile devices are likely to contain vast amounts of sensitive information belonging to both the organisation and the device owner. Whenever mobile devices are compromised the outcome is likely to be severe for the individuals and to the organisations alike. That is why these kinds of devices present a serious IS threat and risk to the crisis preparedness of the information systems within the organisation.

2.1.4.8 Spam

Spam is defined as an unsolicited e-mail which is sent with intent to lure the recipient to buy something or which provides a disproportionately high benefit to the receiver (Goldsborough, 2007; Australian Communications & Media Authority, 2008). Spammers may also use information that is current and interesting to the reader such as political unrest (e.g. the Egypt uprising), the deaths of public figures (e.g. Muammar Gadhafi, Steve Jobs and Amy Winehouse) and natural disasters (e.g. the Japanese tsunami). These are the kinds of topics that newspapers cover and for the same reasons they attract a reader's attention (Symantec, 2012).

The global trends indicate that the overall amount of spam fell considerably in the year from 88.5% of all e-mails in 2010 to 75.1% in 2011 (Symantec, 2012). In part this was a result of the law enforcement action that shut down Rustock, a huge, global botnet that was responsible for distributing large quantities of spam. Despite the fall in e-mail spam, spam remains a chronic problem for many organisations and can pose a silent threat to businesses due to the increase in informational, managerial and operational costs to the organisations. These costs can range from bandwidth costs, productivity losses resulting from wasted time (i.e. time spent to receive, read and delete large quantities of unsolicited e-mails) and money spent on recovering destroyed data (New Zealand Statistics, 2010).

Despite the existence of e-mail filters to reduce the quantity of spam (Goodman, Cormack, & Heckerman, 2007), the increasingly sophisticated techniques used by spammers mean the filters may not prevent users from accessing these spam e-mails. For the same reason, end-users need to be aware of how to identify spam and how to act in case they come across them.

2.1.4.9 Social Media Threats

The attention of online criminals and spammers is now shifting to social media sites (Australian Communications & Media Authority, 2008; Symantec, 2012). The shift is encouraged by the increasing popularity of social networking and micro-blogging sites. The potential of having access to a multitude of people on social networking sites make them attractive targets for online criminals and spammers.

A social media channel (e.g. Facebook and Twitter) is perfect for social engineering as it is easier to trick individuals when they feel they are in safe hands surrounded by friends (Workman, 2008). According to Symantec (2012), over 50% of all attacks identified on social networking web sites were linked to malware infection on compromised Blogs/Web Communications web sites. It is on the social networks that the hyperlinks of the compromised web sites are shared to a wider audience and they are also increasingly used for sending out spam messages. In addition, online criminals are utilizing the power of social media by tricking end-users from different organisations into spreading the compromised links on their behalf.

In order to counteract this challenge organisations are encouraging responsible use of online content and services. This is done by promoting and enforcing policies for responsible behaviour in online communities. These policies encourage end-users to behave reasonably in social media channels and to report those they feel are not abiding to the rules (Australian Communications & Media Authority, 2008).

2.1.5 Challenges to Current Approaches to Crises Situations

As discussed in chapter one, some organisations have committed to a crisis management process (CMP) in order to reduce the severity of potential crises events. Mansor (2004) presents a disaster management cycle of a crisis management process progressing through four phases — mitigation, preparedness, response and recovery (Fig 2.2). The phases of the crisis management process are characterized by different goals and resources (Lettieri, 2009), which means different functions and activities are performed at each phase.

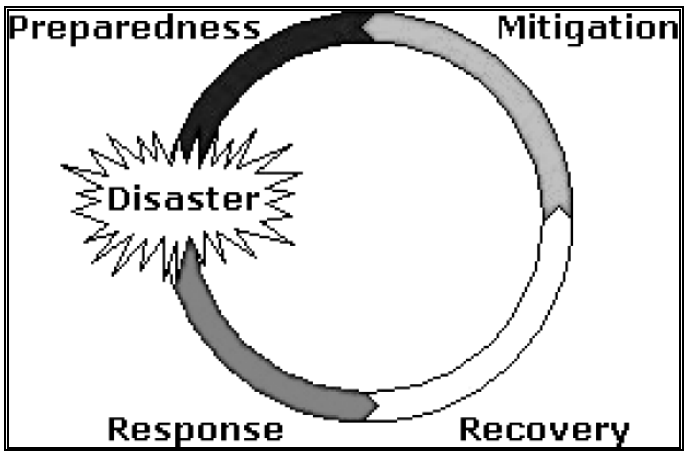

Figure 2.2: Disaster Management Cycle

Source: Shaluf (2008)

Mitigation embraces activities that do away with or reduces the probability and consequences of a disaster, for example, information security measures are established to alleviate the operational risks in order to ensure the dependability of the information systems (Avizienis et al., 2004). The term 'dependability' refers to the ability of the IS platforms to deliver services that can justifiably be trusted. Alternatively, it is the ability to avoid service failures that are more frequent and more severe than is acceptable.

Some of the necessary activities in this phase are to:

- Identify threats and vulnerabilities that might impact the operations of the computing environment;
- Protect the confidentiality, integrity and availability of the information (Allen, 2005).

The mitigation phase also includes the activities performed to establish the components of the business continuity plan (BCP); information systems risk management (ISRM); or information systems security (ISS). In the case of a BCP this can include:

- Business risk and impact analysis;
- Initial tests and training of staff in the business recovery process (Savage, 2002).

Preparedness is defined differently by different authors. From the emergency management perspective, preparedness refers to the development of effective policies, procedures and capacities to plan the best ways to manage a crisis event (Hwacha, 2005). According to Unlu

(2010) preparedness is a process that involves technical tasks, such as the identification of critical resources and the development of the necessary agreements among responding actors (e.g. end-users). Alexander (2005) views preparedness as short-term actions taken to reduce the impact of an impending disaster. Thorough discussion on this concept will follow later.

Response is described as an action undertaken immediately prior to, during and immediately after a crisis or a major emergency (Shaluf, 2008; Hwacha, 2005). Response activities are meant to minimize property damage and enhance the beginning of recovery from the incident (Shaluf, 2008).

Recovery embraces activities that return infrastructural systems to minimum operating standards including guiding long-term efforts designed to return businesses to normal or improved levels after a disaster (Shaluf, 2008). Primarily, this is accomplished through prior strategies established during the mitigation phase, such as business continuity plans (BCPs) or disaster recovery plans (DRPs), and being kept current throughout the preparedness phase,

This study attempts to examine to what degree end-users are aware of and adhere to a range of CPIS measures established within the organisation. In particular, this study focuses on four common approaches applied by diverse organisations to protect their critical business systems running over different IS platforms. They are business continuity plans, disaster recovery plans, information systems risk management and information systems security which was used as a representation of CPIS measures in chapter one. These approaches present different aspects of the CPIS. The number and type of approaches implemented by the organisation depends on the size and the business needs of that particular organisation (Susanto, 2003; Jones, 2007).

Business Continuity Plan (BCP)

A BCP is intended to avoid or mitigate risks; to reduce the impact of a crisis event; and to reduce the time needed to restore critical business systems to a state of "business as usual" (Botha & Solms, 2004; Cerullo & Cerullo, 2004). A BCP is meant to be a dynamic document that must evolve as different changes are introduced in the organisation's business processes (Pinta, 2011). The business continuity planning process is required to address three main interdependent objectives; (1) to identify the major risks that can potentially shut down the computing environment; (2) to develop a plan to mitigate or reduce the impact of the

identified threats and risks; (3) train end-users and then to test the plan to ensure that it works (Cerullo & Cerullo, 2004). To achieve these objectives a number of activities are usually involved. Botha and Solms (2004) present seven phases required to generate a BCP: project planning, business impact analysis (BIA), business continuity strategies, continuity strategies implementation, continuity training, continuity testing, and continuity plan maintenance. Cerullo and Cerullo (2004) group these activities (phases) into three main components of the BCP process: (i) business impact analysis (BIA), (ii) disaster contingency recovery plan, and (iii) training and testing.

For the purpose of explaining the business continuity planning process, this study follows the work of Cerullo and Cerullo (2004). The BIA systematically assesses the potential impacts resulting from different events or situations that may cause critical business systems to be unavailable (Savage, 2002; Botha & Solms, 2004). The BIA process facilitates the organisation to evaluate the risk of business process failures and to identify critical and necessary business functions including the hardware, software, systems, services, and related technology assets that support the organisation's critical operations.

On the other hand, a disaster contingency recovery plan explains procedures to follow when a crisis hits. It lists the names of team members and their specific duties, work-around processes to keep the organisation operational while the damaged IS platforms are being restored to a "business as usual" status. In general, the disaster contingency plan is a critical part of a BCP.

In preparation for potential crises events, training and testing is needed. This is done after completing the BCP (Savage, 2002; Botha & Solms, 2004). Testing of the BCP and related training of the stakeholders are usually followed by auditing the plan at regular intervals. Training and testing are essential to ensure that the BCP is comprehensive to address critical risks (Pinta, 2011). Salvage (2002) observes that training and testing usually only involve the recovery team and exclude other end-users. The lack of involvement of other members of the organisation is due to executives' cost concerns and their perception of business continuity planning as a cost but with no value in return (Cerullo & Cerullo, 2004). This is evident in surveys conducted to examine the status of the BCPs in organisations around the world, which indicate their status to be minimal. For instance, study results published in the Ernst & Young Global Information Security survey (2002) based on responses from 459 Chief

Information Officers and IT Directors from medium to large size organisations worldwide, indicate that only 53% of these organisations had developed a BCP. A similar survey conducted by Meta Group research (2003) as cited by Susanto (2003) shows that only 20% of Global 2000 organisations have effective BCPs to assist them during the recovery phase of a crisis.

Another problem with the current approaches to BCP is that most of the existing BCPs are incomplete and outdated and they don't address today's major risks and threats of business system interruptions (Cerullo & Cerullo, 2004). This might be caused by a lack of knowledge and/or understanding, lack of awareness or failure to adhere to established rules and regulations within the organisation itself, or from the effect of regulatory bodies in the organisational sector. In addition, many of these BCPs have not gone through the normal procedure of carrying out the business impact analysis (BIA) as well as being tested (Ernst & Young, 2002) before their implementation. This could mean a wide gap between what the organisation needs and what the plan can actually provide.

Incomprehensive BCPs in many organisations are also blamed on the lack of participation of active participants in the recovery process (Tootle, 2007; Omar et al., 2011). These are the people knowledgeable or have the understanding of how to deal with crisis events, or are the end-users who use the systems on a day-to-day basis (Nelson, 2006).

Disaster Recovery Plan (DRP)

In some organisations a BCP and a disaster recovery plan (DRP) are considered synonymous (Susanto, 2003), but others view disaster recovery planning as more tightly focused on areas around information systems and services (Watson, 2007; Omar et al., 2011). Nelson (2006) argues that organisations with a BCP usually have a DRP. These two can either be integrated or maintained as separate plans. In essence, the DRP is a technically oriented plan intended to facilitate the recovery of critical business processes so that they are restored to normal operation (Pinta, 2011) after a crisis. "An effective DRP should consist of nine procedural steps: obtaining top management commitment, establishing a planning commitment, performing risk and impact analysis, prioritizing recovery needs, selecting a recovery plan, selecting a vendor and developing agreement, developing and implementing the plan, testing the plan, and continually testing and evaluating the plan" (Chow & Ha, 2009, p. 250). Blatnik (1998), as cited by Chow and Ha, observes that a DRP implementation should consist of nine

stages, namely policy enforcement, threat analysis, back-up strategies, training, testing, documentation, regular reviews, regular updates, and IS staff participation. While Blatnik indicates the necessity of IS staff participation in the DRP implementation, Blatnik, Chow and Ha excluded end-user participation in the process of DRP implementation. That means the DRP may exist in the organisation but it is not brought to the awareness of the end-users. The lack of awareness and no input from end-users is likely to be a source of inefficiency in maintaining this kind of a plan over time.

Similar to the BCP, the DRP is a dynamic document that needs to be updated as new business processes and other new aspects of the business are introduced, and if the organisation learns from tests and operationalisation of plans in response to an actual crisis (Nelson, 2006). With the absence of end-user input the DRP is unlikely to be comprehensive enough to accommodate all potential risks and threats. To address this challenge, Smits and Ally (2003) suggest that organisations should put in place a management infrastructure that assists with creating a behavioural readiness for a crisis via provision of programmes that create awareness and understanding of how crises and interruptions can threaten the organisation's operations and survival.

Information Systems Risk Management (ISRM)

Another important aspect of the CPIS is information systems risk management (ISRM). This is a process of understanding and addressing the factors that may lead to failure in the confidentiality, integrity or availability of critical business systems (Stoneburner, Goguen, & Feringa, 2002). The ISRM process embraces three main stages: initiation, risk analysis and risk mitigation (See figure 2.3). For the purposes of this study, only the risk mitigation stage is reviewed. This is because it is at this stage that end-user involvement becomes important.

Figure 2.3: The Overall Process of Risk Management

According to the ISO/IEC 27001 (2005), the risk mitigation stage (Figure 2.4) consists of three tasks: design, implement, and monitor.

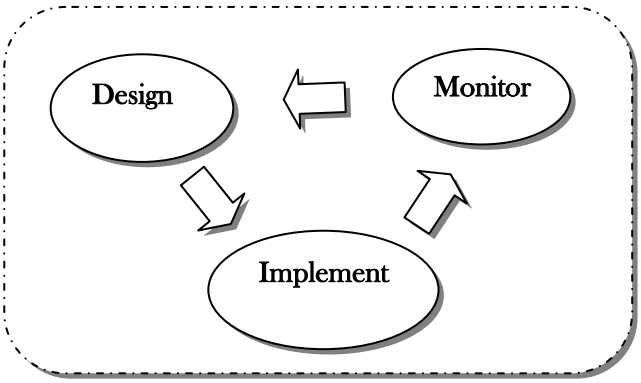

Figure 2.4: Risk Mitigation Stages

The design task embraces the specification of security objectives and the deployment of security policies and processes appropriate for controlling risk. Existing policies and countermeasures are identified and reviewed in comparison to the findings from the risk analysis stage. In the case of any changes, additional control measures are specified and designed, accompanied by the timeframe over which they should be implemented. The implementation task involves the application of the identified control measures and procedures including the management of resources (i.e. people, time, funds, and operations) required for implementing these measures. It is during the implementation stage that security awareness programmes are established in order to build a healthy risk and security culture within the organisation. The final task of the risk mitigation stage is monitoring. This process follows the implementation of the identified control measures and ensures that they are operating effectively and as intended. The monitoring process also includes:

(i) processes for the prompt detection of errors and security incidents;
(ii) mechanisms that examine whether documented procedures are being followed; and
(iii) reviews aimed at the evaluation of implemented controls' efficiency.

Generally, the ISRM process can be improved by addressing the social factors that influence the process and the outcome of the ISRM (Pfleeger, 2000; Gerber & Vonsolms, 2005). The main challenge with ISRM processes is the ambiguity and uncertainty inherent in the risks themselves and the human understanding of how to address them (Pfleeger, 2000). In

common practices, risk analysis focuses mainly on physical elements of the information systems such as the technology, the hardware and the infrastructure. According to Pfleeger, this approach is very unlikely to ensure comprehensive protection of the IS against potential risks and threats. In complementing this argument, Smith (2003) notes that "risk is not fragmented into compartments and silos, risk management should not be either". It is rather recommended that the entire spectrum related to the IS environment is taken into consideration in order to establish a sound and effective ISRM strategy for the organisation. Gerber and Vonsolms (2005), suggest that this approach can be realized by transforming the estimation of threat and risk analysis to include the social aspects of the CPIS. In other words, ISRM processes can be organised so that they take into account the values, beliefs, and biases (Pfleeger, 2000; Gerber & Vonsolms, 2005) of those affected by the CPIS within the organisation. What is being referred to here is the need to evaluate IS threats and risks based on values, beliefs and biases of the end-users in addition to the technical approach. These social aspects which are influenced by factors such as history, culture, politics, law and religion (Gerber & Vonsolms, 2005) are likely to affect the social context of security controls' application and the stakeholders' perceptions with regard to IS threats and risks (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2006). In many cases risk depends on a complex interplay of different social variables, which are influenced by human judgment. Again, the identification and estimation of risk is both a human and a social activity. Karyda et al., (2004) as cited by Tsohou (2006), observe that ISRM is affected by organisational elements, including social and cultural aspects.

The point above is well explained by cases whereby end-users are not aware of the security measures put in place by their organisations (Cerullo & Cerullo, 2004; Tsohou et al., 2006). In such circumstances IS security measures are viewed as bottlenecks (i.e. time wasters) rather than a necessity (Smith & Jamieson, 2006). In order to change this attitude and allow for end-users to comply with established CPIS measures, some organisations have introduced training and awareness programmes. However, apart from awareness and training there are other social factors that affect end-users' perceptions of IS threats (Tsohou et al., 2006). This is the reason why there is much diversity in the way end-users and other stakeholders react to different risks and threats. Their thoughts of IS risks and threats may result from personal experience, from what they have seen or heard in the mass-media (e.g. newspapers, internet, TV, etc.) or from what they have learnt from friends. According to Tsohou et al., (2006) other

social factors that influence end-users' perceptions include their familiarity with the source of danger, their ability to control the situation, and the severity of the crisis event.

On the other hand, end-users are unlikely to follow organisational information security guidelines appropriately even though they are aware of them (Siponen, 2000). This is because ISRM involves a number of human activities that depend on how end-users perceive risk with regard to IS. To explain this phenomenon, Tsohou et al., (2006), observe that people tend to evaluate risks differently when they rate the same risks for themselves, their family, and people in general. This could be the main reason of disparity between the end-users' ranking of threats and those of IS security professionals. This point of view is also supported by Rippl (2002), who argues that individuals are embedded in a social structure that acts like a filter shaping their values and attitudes [with regard to IS risks].

Despite the existence of several ways to minimize the negative impact of crises events, unfortunately the literature shows these methods have failed to produce the intended results. Problems mentioned in this text are not exhaustive; however they indicate that many of the difficulties and shortcomings revolve around lack of understanding, lack of awareness and failure to adhere to CPIS measures by the users of the information systems.

2.2 Crisis Preparedness

Failures in crisis preparedness of the information systems (CPIS) endeavours have been linked to inadequate business and risk strategies, inadequately informed decision-making based on insufficient information and lack of appropriate authorisation from senior management. The situation is often intensified by the deficiency of clearly defined risk limits, intentionally misleading reports, insufficient intra-organisational communication concerning risk vulnerability, shallow or unrealistic risk control measures, poor knowledge of the business environment and lack of timely decision-making (Eaglestone et al., 2003). The seriousness of the matter becomes even more pressing as organisations depend on a zero-defect quality IS to facilitate their critical operations (Applegate, 1999). The survival of the IS platforms can be equated to the existence of the organisation itself (Susanto, 2003). This point of view can be rephrased to mean that "an organisation will only prevail as long as it's IS platforms remain operational" during and post the crisis event.

The IS platforms within an organisation can be sustained throughout a crisis event by implementing comprehensive measures for the CPIS. However, organisations are likely to ignore the warning signs or triggers of an impending crisis due to over-dependence on the existence of protection or preventive measures (Caponigro, 2000) for IS. This dilemma is well explained by Pollard and Hotho (2006), asserting that plans, such as contingency planning, BCP or ISRM are likely to create a false sense of preparedness where in actual fact it does not exist.

It might be worthwhile to consider similar attempts at CPIS used by the Association of peri-Operative Registered Nurses (AORN) to check their preparedness status: "Are you prepared? Is crisis planning part of your orientation plan for (staff) new to your department? We prepare our staff to operate with high-tech equipment, but would they also know how to function in a low-tech situation?"(Steiert, 2007, p. 175) It is a common phenomenon in many organisations, after accomplishing the development of so called "plans" such as BCP, DRP or ISRM, to feel a sense of security. Regrettably, many such plans are placed on a bookshelf or shoved in a file drawer and forgotten. In fact, some organisations did prepare some of these plans but, during an actual crisis, came to realize that they never thought of or considered the plans they had prepared (Caponigro, 2000). This study finds out the degree to which some of these challenges have been addressed in New Zealand organisations in order to avoid similar traps (issues) as highlighted in the extant literature.

2.2.1 Understanding the Concepts of Crisis Preparedness

In principle, 'crisis preparedness' activities involve preparing for what has not yet occurred. There are two similar concepts in relation to crisis preparedness: readiness and willingness. The comparable nature of these concepts is drawn from their usage in various research studies. In fact, some authors have gone further to use the terms interchangeably. In conceptual terms, readiness is similar to preparedness in the effectiveness literature (Banerjee & Gillespie, 1994). Many such studies focus on some type of accidents, errors, destabilizing event or uncertainty (Perrow, 1999) when referring to potential threats to IS assets. On the other hand, willingness embraces behavioural features of people such as attitudes and wishes. These behaviours can manifest themselves at any level of the undertaking—at the individual level, at the departmental level, or at the organisational level.

2.2.1.1 Readiness

Gillespie and Streeter (1987, p. 156), define readiness as the "degree of readiness to deliver services in response to a disaster. Rousaki and Alcott (2006) broadly define crisis-readiness as the capability to cope with the uncertainty caused by a crisis. From a different perspective, Reilly (1993) suggests that crisis-readiness activities should incorporate both crisis prevention and crisis management components. Prevention refers to technology and people engaged in activities to reduce vulnerability to a crisis, whereas a crisis management component involves responding to a crisis. Reilly (1993) further suggests that the execution of crisis management requires capabilities in decision response, information flow — both internal and external, and implementation, as well as resource mobilization. Drawing upon the same understanding, Smits and Ezzat (2003) argue that leadership and team-building are central elements in the effective handling of a crisis and they point to the importance of a meaningful human infrastructure development.

By and large, readiness— similar to preparedness— embraces fundamental concepts associated with effectiveness. They include effective mobilization and allocation of scarce resources, communication among stakeholders, as well as effective dissemination of information to key stakeholders. In addition, readiness involves coordination and utilization of key capabilities in handling crisis events.

2.2.1.2 Willingness

One of the requirements in ISO 27001:2005, "Information technology — information security management systems" advocates the value of implementing and operating controls to manage an organisation's information security risks. In best practices, information security risks must be managed in the context of the organisation's overall business risks. There are diverse ways in which risks and threats can be handled at the organisation level. The differences in approaches depend very much on the type of the organisation and its 'risk appetite'— the extent of its willingness to accept risk. As Jones (2007) puts it "some will embrace risk where they feel that it offers the opportunity for greater reward, while others are more conservative and will be considered risk averse".

Willingness is also embraced in issues of organisational politics. Political will is an essential feature for sustained efforts in risk reduction (UN/ISDR, 2002). Gaining political

commitment from those in authority has a positive influence on activities intended to reduce negative impacts of crises. Political willingness is significantly important in giving crisis-preparedness the place it deserves. Despite the necessity of commitment from those in authority, other elements such as the mobilization of human, technical, material and financial resources (Broadbent & Weill, 1997; Armstrong & Sambamurthy, 1999; Smaltz, Sambamurthy, & Agarwal, 2006) are pertinent to meet the expectations that CPIS can provide.

Some stakeholders have the perception that crises are unexpected, unplanned, and just Acts of God. To them, planning and committing high costs in order to prepare for such events becomes less important. Thus, inadequate preparedness can relate both to unwillingness and inability to prepare (Kusumasari, Alam, & Siddiqui, 2010).

Individual willingness can be demonstrated in situations where end-users are required to update different software applications on their working stations by pressing the update button. Since this action is voluntary it will take individual willingness to click the update button in order to apply the required patches to the software application. This can also happen the other way round, where a pop up window from malicious software is displayed on the screen asking end-users to click on it in order to download and install. The judgement made by some end-users on which action to take will very much depend on their willingness to protect or harm (Garrett, 2004) regardless of their understanding or awareness of the consequences of their actions (Tsohou et al., 2006) to the information systems in that particular organisation.

2.2.2 Crisis-Preparedness Defined

The term “preparedness” is defined variously in the literature. Research studies from the public health sector sought to establish a comprehensive definition that could articulate the needs and the key elements that characterise a well-prepared community (Nelson et al., 2007). The established definition focuses on situations “whose scale, timing, or unpredictability threatens to overwhelm routine capabilities of the community (Nelson et al., 2007, p. S9)”. The process of crisis-preparedness is not a steady state; it involves continuous improvements, including frequent testing of plans through drills and exercises, and the formulation and execution of corrective action plans (Shaluf, 2008). Lack of these elements seem to be the source of many of the challenges associated with failures in crisis

preparedness strategies such as business continuity planning (BCP) and information systems risk management (ISRM). For instance, the BCP is not a document prepared as a one-off event and put on the shelf (Savage, 2002; Smith & Jamieson, 2006), rather it should be dynamic and must involve the active involvement of the top management team, IS staff, and IS-users (end-users). This is necessary to ensure constant updating and testing by accommodating inputs from all key participants. Active participation of all end-users is necessary to allow for understanding, awareness of, and adherence to established CPIS measures within the organisation.

Again, crisis-preparedness can be explained as including certain capabilities such as the ability to build and apply IS, the ability to recognise signals and the ability to see the big picture regarding crises (Leidner, Pan, & Pan, 2009). However, capacity alone does not ensure preparedness (Nelson et al., 2007). This standpoint resonates through Wood's (1995) argument, which gives a caution on directing much attention to the technology alone when dealing with information security issues. The ability to build, apply and recognise signals requires other capacities such as good infrastructure, trained personnel, and proper planning. Nelson et al., suggest that crisis-preparedness must involve a coordinated and continuous process of planning and implementation that relies on measuring performance and taking corrective action. For instance, when people change jobs, in many instances it is very difficult to maintain the collection of knowledge to sustain safety and effective operations of critical business systems (Smith & Jamieson, 2006). This is because when a new employee joins an organisation he/she will most likely be oriented through operational processes while ignoring other pertinent processes such as security and recovery of business systems (Smith & Jamieson, 2006). This state of affairs will put all critical business processes at high risk regardless of their technological capacity.

Moreover, crisis-preparedness can be explained based on the activities performed or ignored. Mitroff, Pauchant, Finney and Pearson (1989) contend that being crisis-prepared or crisis-prone can be drawn on the activities and structures to avert or decrease the damages inherent in potential crises. Structures associated with crisis-preparedness are characterised by effective audits, prearranged actions, and policies aimed at forecasting potential crisis occurrences (Greening & Johnson, 1996; Shrivastava, 1993). On the other hand, crisis proneness is the opposite state, in which none of the above aspects exist, possibly leading to an unconscious or negligent vulnerability to crisis events (Pollard & Hotho, 2006).

This discussion on preparedness, readiness and willingness accompanied by a few examples highlighting crisis-preparedness concepts, allows us to define the term "crisis-preparedness" of the information systems. Therefore, for the purposes of this study, crisis-preparedness of the information systems is defined as:

A degree to which end-users are aware of the activities, policies and procedures such that are able to immediately address adverse circumstances that have the potential to develop into information systems crises.

2.3. The Information Systems

2.3.1 Introduction

The preceding sections elaborated in detail the nature of a crisis and the concept of crisis preparedness in the context of information systems. This section briefly explains the domain of IS and how it relates to the other two concepts in this study.

2.3.2 The Significance of the Information Systems

The significance of the information systems (IS) is made evident by their applications to a wide array of business processes and activities within and outside the organisation. Several studies that exemplify the importance of IS exist in literature. Some of them demonstrate the role of IS in facilitating innovation and business performance (Bharadwaj, 2000). This has also created a belief that IS is fundamental to the organisation's growth and survival. The contribution of IS towards business performance is extended further to include it as a positioning strategy for the organisation in a particular market segment and count as a key resource against its competitors (Rivard, Raymond, & Verreault, 2006). It is important to recognise that in a current business environment whether it is a business activity or a business process both are highly dependent on the organisational IS of which the complexity and advancement depends on the size of the organisation (Chang & King, 2005).

While the potential benefits realised from being crisis prepared are evident from the literature (Parnell et al., 2010), drawing upon them has proved to be a challenging task for many organisations. Considering the high occurrence of crises and the increased dependence on IS

in organisations, one would assume that most firms would have established concrete measures to counteract these events. However, the literature indicates otherwise. There are many factors contributing to this state of affairs such as (1) end-user non compliance with many of the established regulations, policies and procedures to protect the information systems of the organisation (Stanton, Stam, Mastrangelo, & Jolton, 2005; Pahnila et al., 2007a), (2) lack of end-user awareness of the many tools and resources available to them to act accordingly to a given event (Aytes & Conolly, 2003; Pinta, 2011), (3) acts of neglect, and (4) the thoughts that CPIS responsibilities belong to a special group of people.

Confronted with this reality, this study investigates the extent to which end-users are aware of, and to what degree are able to put into practice different measures meant to protect the information systems of the organisation from potentially adverse events. The essence of keeping the IS up and running is emphasised by the fact that organisations that are unprepared for potential IS threats and risks are likely to experience huge damages (Mitroff, 2005) if crises occur, and if they successfully transcend a crisis event it can be considered to be only a matter of chance (Mayer, Moss, & Dale, 2008; Smits & Ally, 2003).

2.4. Theoretical Foundations of the CPIS

A number of measures exist to address several concerns in connection to CPIS challenges. These efforts range from implementation of policy compliance measures, training and awareness programmes, and enforcement approaches such as IS usage regulations, IS security policies and email/Internet etiquette (Australian Communications & Media Authority, 2008). However, two concerns have been raised on the extant awareness approaches. Some studies e.g. Puhakainen (2006), Aytes and Conolly (2003) and Siponen and Oinas-Kukkonen (2007) indicate that (1) current awareness methods lack theoretical grounding, and (2) the absence of empirical evidence to demonstrate their effectiveness. Despite these observations, awareness, training and enforcement approaches with regard to CPIS remain dominant in many of the IS publications.

Human behaviour is a crucial subject for the CPIS effectiveness. Nonetheless, little can be found from the published research on why end-users so often take on unsafe computing practices. This also includes how their behaviour could be modified in a positive way (Aytes & Conolly, 2003) to align to CPIS expectations. According to Siponen (2000), many of the efforts directed to user training and awareness focus on instituting standards related to

knowledge and skills. These training resources, however, miss out on ensuring learning, as they do not take into account behavioural theories linked to learning and motivation (Siponen, 2000; Siponen, 2006). While ensuring learning for end-users remains outside the scope of this study, but this study employs theories related to attitude, motivation, and behaviour in order to understand the extent of user awareness of, and adherence to crisis preparedness of the information systems in New Zealand organisations. As thus, two theoretical frameworks are identified as providing a sound basis to lead this investigation: the Theory of Reasoned Action (TRA) and the Protection Motivation Theory (PMT).

2.4.1 Integration of the Theoretical Models

This study integrates the Theory of Reasoned Action and Protection Motivation Theory. This follows a thorough review of the relevant literature on business continuity; data recovery; IS risk management; IS security; and general IS. Many of these studies e.g. Pahnila et al., (2007a), Lippert and Volkmar (2007), Aytes and Conolly (2003) used these two theories in combination with other theories to investigate and/or evaluate human behaviour, prevention behaviour and control behaviour with respect to IS applications from different organisational settings.

2.4.1.1 Theory of Reasoned Action

The Theory of Reasoned Action (TRA) (Fig. 2.5), which was formulated by Ajzen and Fishbein (1980), has its origin in the field of social psychology. The core assumption of the TRA proposes that an individual's behaviour is determined by his/her intention to perform the behaviour and that this intention is, in turn, affected by the views of others within his/her social setting. The authors further assert that behaviour is best predicted by the intention. Intention is the cognitive illustration of an individual's readiness to carry out a given behaviour, and it is considered to be a direct precursor of the behaviour. Behaviour is the transition of intention into actual action. This intention is a function of the individual's attitude towards the specific behaviour and his/her subjective norms (i.e. normative beliefs in TRA). This argument draws from the fact that the TRA model usually focuses on the determinants and performance of a single behaviour (Sheppard, Hartwick, & Warshaw, 1988). Ajzen and Fishbein (1980) argue that disregarding the likelihood of selecting from alternative behaviours represents a serious omission in the model.

In a computing environment end-users are constantly faced with a choice among policies, regulations, procedures, commands, and actions. In such situations in which individuals are forced to opt among alternative behaviours their thoughts and feelings toward alternative behaviour are influenced (if they have any influence at all) through their effect on individuals' attitudes and subjective norms toward the particular behaviour of interest. As such attitudes, subjective norms, and intentions toward particular behaviour are fundamental in any attempt to deploy the TRA in assessing a given behaviour. Sheppard et al., (1988) postulate that the more positive such factors are, the more likely it is that individuals will perform the behaviour.

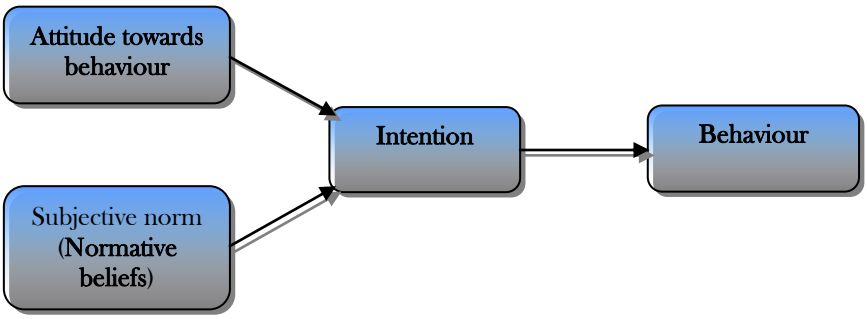

Figure 2.5: Theory of Reasoned Action Model

Source: Fishbein (1980)

Attitude

Attitudes embrace the beliefs an individual acquires through direct experience, outside information, and self generated conclusions (Lippert & Volkmar, 2007). An attitude is an individual's belief about whether the result of his/her action will be constructive or destructive. An individual is said to possess a positive attitude toward the behaviour only if he/she has affirming beliefs about the result of his/her behaviour. Attitude is considered to be more static and internalized (i.e. lasts from months to years) and it is mainly linked to the quality of actions (Siponen, 2000). In the context of this study, the satisfying of the attitude factor means that the consequences of carrying out the measures for the crisis preparedness of the information systems (CPIS) must be desirable. This results in research hypothesis 1:

Research hypothesis 1*(H1)*:

End-users' intention to comply with the measures for CPIS within the organisation is likely to be positively influenced by their attitude of crisis preparedness of the information systems.

Normative beliefs

Normative beliefs embrace normative expectations of peers, superiors and colleagues which may have a persuasive influence on an individual to either perform or not to perform a specific behaviour norm (Ajzen, 1991). With regard to crisis preparedness of the information systems (CPIS), normative beliefs may refer to different policies, regulations or standards that the management expect to be followed by every member of the organisation. According to Aydin and Rice (1991), the behaviour of individuals is an outcome of the interaction that goes on among the members of a given community. Thus, belonging to a certain social setting or being exposed to the influence of important people may have a persuasive influence on whether an individual either performs or does not perform a specific behaviour. In the context of this study, IS staff, IS managers' or senior managers' behaviour toward complying with established CPIS measures will have a persuasive effect on end-users' adherence to CPIS. This allows the generation of research hypothesis 2:

Research hypothesis 2*(H2)*:

Normative expectations about the crisis preparedness of the information systems are likely to affect end-users' intentions to comply with the measures for CPIS within the organisation.

Intention

Two more elements are drawn from the TRA: the intention to comply and actual compliance with CPIS measures. Ajzen (1991), suggests that intentions capture the motivational factors that have an influence on individual behaviour, and they demonstrate the difficulty individuals are willing to accept to perform the behaviour in question. In terms of TRA, the stronger the intention to commit oneself to a form of behaviour, the more likely the behaviour will be performed. In the context of this study, the satisfying of the intention factor means that the stronger the intention to comply with CPIS measures, the more likely the end-users

will actually comply with the established measures for the CPIS. According to Rogers and Prentice-Dunn (1990), intentions serve as the most appropriate measure of protection motivation, as applies to end-user adherence to CPIS for this particular study. This is also reflected in previous research on technology acceptance that says intentions are good predictors of actual behaviour (Venkatesh, Morris, Davis, & Davis, 2003). This allows the generation of research hypothesis 3:

Research hypothesis 3*(H3)*:

End-users' intentions to comply with CPIS measures are likely to have a significant impact on actual compliance with CPIS measures.

2.4.1.2 Protection Motivation Theory

At first the Protection Motivation Theory (PMT) was developed to explain the effects of fear appeals on health attitudes and behaviours (Rogers, 1975). The theory was revised (Maddux & Rogers, 1983) into an all-purpose theory of persuasive communication, with much attention given to cognitive processes mediating behavioural change. A revised version of PMT has allowed its applicability to a diverse array of topics, including areas of interest beyond health-related issues (Floyd, Prentice-Dunn, & Rogers, 2000). In addition to influencing and predicting various health behaviours, PMT has been extended to information systems security (Pahnila, Siponen, & Mahmood, 2007b), effects of technology on culture (Lippert & Volkmar, 2007) and behavioural change in earthquake preparedness (Mulilis & Lippa, 1990). Floyd et al., (2000), suggest that the PMT is an appropriate framework to study situations that involve threats for which there is an effective recommended response that can be carried out by the individual— end-users in the context of this study. The PMT endorses the idea that motivation toward protection results from a perceived threat and the need to avoid the potential negative outcome (Floyd et al., 2000). This is because end-users in an IS environment are constantly faced with a decision to weigh the costs of taking the protective action against the expected benefits of taking that action.

The PMT (Figure 2.6) is structured along two processes that aim to mirror the cognitive processes that individuals use in assessing threats (i.e. a threat-appraisal process) and in choosing among coping alternatives (i.e. a coping-appraisal process) (Floyd et al., 2000). The product of these appraisal-mediating processes is the decision (or intention) to start, maintain, or hold back to the recommended adaptive responses. In essence, intentions indicate the

effectiveness of the attempted persuasion to follow the communicator's recommendations. For the same reasons, dependent variables drawn from the PMT provide key measures for the behavioural intentions (Mulilis & Lippa, 1990) of the end-users toward crisis preparedness of the information systems.

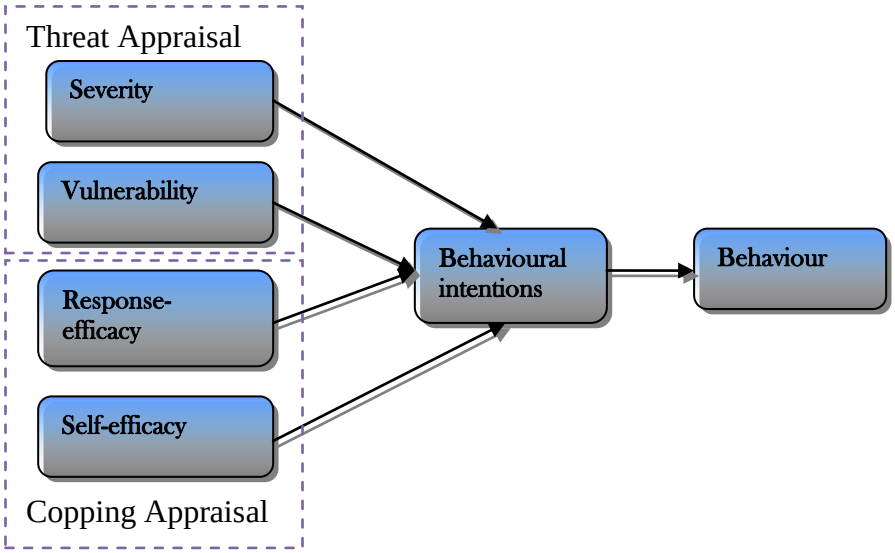

Figure 2.6: Protection Motivation Theory Model

Source: Maddux and Rogers (1983)

Threat appraisal

Threat appraisal consists of two dimensions: perceived vulnerability and perceived severity (Woon, Tan, & Low, 2005). Perceived vulnerability is a conditional probability that a negative event will occur if no measures are taken to counter it (Rippetoe & Rogers, 1987). In the context of this study, the negative event encompass all sorts of IS risks and threats that can potentially damage or shutdown the computing environment of the organisation. This study draws on the concept of perceived vulnerability to refer to end-users' perceived assessment of whether their organisation is vulnerable to IS risks and threats, and the imminence of such threats if no correct measures are carried out to offset them. The assumption being made here is that if end-users do not realize that they are truly confronted by IS risks and threats, they are unlikely to comply with the measures for the crisis preparedness of the information systems (CPIS). Rippetoe and Rogers (1987) refer to perceived severity as both psychological and physical harm the threat can cause. From the standpoint of this study, the perceived severity represents impending negative outcomes with

a root cause due to non compliance with the measures for the CPIS. Again, the assumption here is that if end-users do not see that they are actually confronted by IS risks and threats and if they do not believe that these threats can develop into negative consequences for the organisation, they will barely comply with the established measures for the CPIS. This leads to research hypothesis 4:

Research hypothesis 4*(H4)*:

Threat appraisal affects end-users' intention to comply with established measures for CPIS within the organisation.

Coping appraisal

Coping appraisal embraces three dimensions: response efficacy, self efficacy, and response cost (Rippetoe & Rogers, 1987; Woon et al., 2005). However, for the purpose of this study, response cost is considered irrelevant since all cost resulting from end-user behaviour will be covered by the employer. According to Pahnila et al., (2007b), response efficacy relates to the belief in the perceived benefits of the action. That means, performing a coping action may offset the potential threat. In the context of this study, this could imply that end-user adherence to crisis preparedness of the information systems is an effective approach to identify potential IS risks and threats. Self-efficacy focuses on the individual's ability, or judgment of their capabilities, to cope with the task at hand or in sight (Bandura, 1977). The self-efficacy concept is built on the assumption that if organisations can increase employees' self-efficacy, judgment about their abilities to cope well with the tasks in sight can improve their efficiency. In the context of this study, it all comes to the end-users' beliefs on whether their actions towards established CPIS measures will actually lead to adherence to these measures. Maddux and Rogers (1983) contend that self-efficacy is the most dominant predictor of intention. This leads to the generation of research hypotheses 5 and 6:

Research hypothesis 5*(H5)*:

Response efficacy affects end-users' intentions to comply with established measures for CPIS within the organisation.

Research hypothesis 6*(H6)*:

Self-efficacy affects end-users' intentions to comply with established measures for CPIS within the organisation.

Crisis Preparedness Awareness

Crisis preparedness awareness is a measure adapted for this study to measure the extent to which end-users' understanding and knowledge of their roles and responsibilities, IS standards, organisational regulations, and processes to protect, to prevent and to manage the information systems threats and risks are important to the actual compliance with the measures for the crisis preparedness of the information systems. This measure draws upon various facts from IS security effectiveness. Different scholars, e.g. Aytes and Conolly (2003), Al-Zarouni (2006), Australian Communications and Media (2008), and Tetmeyer and Saiedian (2010) assert that training and awareness are necessary antecedents to the effective use of countermeasures. In the context of this study, countermeasures refer to different aspects of crisis preparedness of the information systems within the organisation. This study draws on the argument that training and awareness are fundamental for the effectiveness of security countermeasures. This argument also suggests that end-user behaviour is the result of two key factors: awareness that threats exist, and training in the proper use of countermeasures (Aytes & Conolly, 2003). This point of view assumes that much of the training content will ensure that end-users are aware of organisational policies and procedures related to countermeasure use. It also assumes that either users will inherently be motivated to comply with these policies, or compliance can be mandated. This results in the generation of research hypothesis 7:

Research hypothesis 7*(H7)*:

Crisis preparedness awareness positively influences end-users' intentions to comply with established measures for CPIS within the organisations.

Therefore, this study tests seven research hypotheses (see Table 2.2) in order to understand the extent of end user awareness of and adherence to crisis preparedness of the information systems in New Zealand organisations.

Table 2.2: Research Hypotheses with their Respective Theoretical Foundations

SN	Research Hypotheses	Theoretical Foundation	Source
1	End-users' intention to comply with the measures for CPIS within the organisation is likely to be positively influenced by their attitude of crisis preparedness of the information systems.	TRA	Ajzen and Fishbein (1980); Sheppard et al., (1988) Siponen, Lippert and Volkmar (2007)
2	Normative expectations about the crisis preparedness of the information systems are likely to affect end-users' intentions to comply with measures for CPIS within the organisation.	TRA	Ajzen and Fishbein (1980); Sheppard et al., (1988) Siponen, Lippert and Volkmar (2007)
3	End-users' intentions to comply with CPIS measures are likely to have a significant impact on actual compliance with CPIS measures.	TRA	Ajzen and Fishbein (1980); Sheppard et al., (1988) Siponen, Lippert and Volkmar (2007)
4	Threat appraisal affects end-users' intention to comply with established measures for CPIS within the organisation.	PMT	Maddux and Rogers (1983); Rippetoe and Rogers (1987); Floyd et al., (2000); Woon et al., (2005) ;Lippert and Volkmar (2007); Pahnila et al., (2007b)
5	Response efficacy affects end-users' intentions to comply with established measures for CPIS within the organisation.	PMT	Maddux and Rogers (1983); Rippetoe and Rogers (1987); Floyd et al., (2000); Woon et al., (2005) ;Lippert and Volkmar (2007); Pahnila et al., (2007b)
6	Self-efficacy affects end-users' intentions to comply with established measures for CPIS within the organisation.	PMT	Maddux and Rogers (1983); Rippetoe and Rogers (1987); Floyd et al., (2000); Woon et al., (2005) ;Lippert and Volkmar (2007); Pahnila et al., (2007b)
7	Crisis preparedness awareness positively influences end-users' intentions to comply with established measures for CPIS within the organisations.	Adapted for this study	Aytes and Conolly (2003); Al-Zarouni (2006); Australian Communications and Media Authority (2008); Yuan and Jang (2008); Tetmeyer and Saiedian (2010)

Key: **TRA**-Theory of Reasoned Action, **PMT**- Protection Motivation Theory

2.5 Chapter Summary

The literature review had the purpose of establishing the theoretical foundations of this research. Given the number of challenges associated with the CPIS, it was essential to review relevant literature about the nature of crises, crisis preparedness, and the information systems.

From section 2.1.1 to section 2.1.5 the review explored the general understanding of crises with respect to the information systems. From these sections the reader is able to capture the

general perspective of crises with regard to the IS environment. The "crisis" object is defined followed by a review of common IS risks and threats in New Zealand organisations. This block is completed by a discussion on various challenges to current management approaches to crises.

Section 2.2 reviewed and discussed the "preparedness" concepts. In this section crisis-preparedness and related concepts are presented followed by a discussion which defines the crisis preparedness of the information systems.

Section 2.3 explored and discussed the significance of the IS in the organisational setting.

Section 2.4 reviewed two theoretical foundations— the Theory of Reasoned Action and the Protection Motivation Theory. The review of the theoretical foundations allowed for the generation of the seven research hypotheses.

Chapter 3: Research Design and Methodology

3.1 Introduction

Research design provides a structure according to which the research will be conducted. This chapter presents the underlying assumptions that guided this study, followed by the research design chosen in an attempt to answer the research question(s). Methods and strategies used in collecting and analysing data are also presented followed by the process of validating the instruments. Finally, ethical considerations followed by this study are presented.

3.2 Research Paradigm

The aim of the research methodology was to produce an instrument that would explore the topic of the research and describe the crisis preparedness of the information systems phenomenon (Guba & Lincoln, 1994; Myers, 1997; Creswell, 2003) in New Zealand organisations. The description of the phenomenon pertained to end-user awareness of and adherence to crisis preparedness of the information systems. This study was conducted from a positivist research perspective based on the ontological assumption that reality is external and objective (Hirschheim, 1992). It assumes that the universe consists of objectively given, immutable objects and structures. These exist as empirical entities, on their own, independent of the observer's appreciation of them.

In the context of this study, crisis preparedness of the information systems is a single standing reality that doesn't depend on how different individuals view it. As an example, the structure, the capability and functionality of the protection mechanisms for critical business systems against IS threats and risks exist in the organisation. These features won't change regardless of how you look at them— that is the reality. This scenario demonstrates the relevance of using the positivist perspective as an investigative paradigm. This is because it assumes that reality is objectively given. Since objectivity does not depend on individual standpoints it allowed the use of a survey instrument to capture end-users' perceptions. This is because survey data can be collected by using quantifiable measures and thus can be explained by measurable properties which are independent of the observer (Orlikowski & Baroudi, 1991; Ponterotto, 2005; Gregor, 2006).

In social science research, it is assumed that methods are tied to paradigms (Landry & Banville, 1992; Mingers, 2003). This sentiment concurs with the argument made by Orlikowski and Baroudi (1991), suggesting that research methods develop within a particular paradigm. In line with the positivist philosophy and its underlying assumption that "reality is objectively given and can be explained by measurable properties which are independent of the observer" (Ponterotto, 2005; Gregor, 2006), a quantitative method was indicated.

3.3 Research Methodology

A research methodology is a path used by the researcher in pursuit of answers to the research question(s) (Kumar, 2005). The path is comprised of a number of steps and procedures that a researcher follows. The steps and procedures of the research methodology may include the following: (1) the collection of quantifiable information through self-reporting of study participants (Polkinghorne, 2005) or quantitative methods; (2) the use of case studies, interviews, and ethnographic methods— the qualitative methods (Denzin & Lincoln, 2005); or (3) the utilization of mixed methods (i.e. combining qualitative and quantitative approaches) which may run in parallel, concurrently or sequentially (Östlund, Kidd, Wengström, & Rowa-Dewar, 2011). The existence of a multiplicity of methods, procedures and models of research methodology made it necessary to choose an appropriate method that ensured the objectives of the study were attained (Hanson, Creswell, Plano Clark, Petska, & Creswell, 2005).

Because crisis preparedness of the information systems is a single reality that can objectively be explained it was possible to use quantifiable measures to answer the research question(s). Therefore, for this reason and in consideration of the positivist assumptions and the objectives of this study, a quantitative method was adopted.

3.3.1 Quantitative Methods

Quantitative positivist research embraces a set of methods and techniques that allow the researcher to provide answers to the research questions (Straub, Gefen, & Boudreau, 2005). After first identifying the research variables, the generation of research hypotheses follows. The next step was the creation of items which were later used as questionnaire questions to seek for opinions or perceptions from end-users of the information systems in organisations. By using the deductive approach, the researcher was able to get a broader understanding

(Helms et al., 2006; Morrow, 2007) of the CPIS phenomenon in New Zealand organisations. This was made possible by examining through the data again and again (Ponterotto, 2005).

In general, a quantitative study seeks out facts or causes of certain phenomena without requiring subjective interpretation. Subjectivity is avoided by minimising personal prejudice and bias. This was necessary to ensure that a social setting in the surveyed organisations is presented as it is, rather than as it is imagined by the researcher. Moreover, this study applied a descriptive type of quantitative research in order to accomplish the research objectives (Pinsonneault & Kraemer, 1993). A descriptive study promises statistically sound results if a large number of respondents agree to participate in the study. This is pertinent to generate findings which are generalisable to the whole population (Kaplan & Duchon, 1988; Straub et al., 2000).

3.4 Data Collection and Analysis

In the existing social science literature there are mostly two types of data collection methods: surveys and interviews. The decision on which method to use is essentially grounded on the theme of the study. For theory-testing methodologies, surveys and experiments are the leading methods in social science research. However, field interviews and in-depth case studies remain predominant for researchers intending to develop a theory (Alam, 2005).

This study drew on the descriptive aspect of quantitative research. In order to attain conclusive results descriptive analysis requires a large quantity of quantitative data. This data was collected through an online survey made accessible to intended participants over the Internet. Since data analysis in this study was inspired by descriptive questions, it means the study ascertained facts about CPIS through theory testing (Pinsonneault & Kraemer, 1993).

3.4.1 Online Survey

The collection of quantitative data commenced once the instrument and the measures were comprehensively tested for validity and reliability. By using the New Zealand Companies Office Register sixteen organisations were identified as potential data collection sources. These companies were selected from different sectors: Energy, Telecommunication, Banking, Information Technology, Tertiary education and service industries. According to the data hosted by the Companies Office Register, the number of employees from the identified

organisations ranged from 500 to 10,000. The large numbers of employees provided a potential source for large quantity of respondents to take part in the survey (Web-based survey) (Pinsonneault & Kraemer, 1993; Hair et al., 1995; Boudreau et al., 2004). This was based on the fact that a large sample size would provide for stronger external validity and streamline the examination of the hypothesised relationships (Pinsonneault & Kraemer, 1993). Inadequate sample size had the potential to cause serious problems in the course of analysing data and hypotheses testing (Boudreau, Gefen, & Straub, 2001; Straub et al., 2005).

The quantitative approach was descriptive. It encompassed an organisation-wide Web-based survey. The choice of a web survey was based on benefits it would offer to the researcher in order to make the study successful (Straub, Gefen, & Boudreau, 2005). The Web-based survey contained a self-administered questionnaire accessible via a standard web browser. The invitation to participate in the survey was sent to potential respondents via their e-mail addresses. In order to protect participants' anonymity, the participating organisation(s) offered to help with the distribution of the survey web-link. A representative from the communication or the IT/IS department in those organisations distributed the survey web-link including a short cover letter (survey instructions) to participants' email accounts. The completed questionnaires were submitted back to the researcher through the Qualtrics survey application, and no identifying data was present in the returned surveys.

The Web-based questionnaire covered seven key areas: (a) basic demographic information, (b) general understanding of the subject of crisis preparedness of the information systems (CPIS), (c) CPIS duties and responsibilities, (d) end-user's awareness of the fundamental aspects of CPIS including processes and procedures, (e) end-user's understanding on IS threats and risks and their outcome, (f) end-user's involvement in training and awareness programmes, and (g) end-user's intentions and reaction to CPIS improvements and changes. The Web-based survey presented some major difficulties to the researcher such as low response rate and non-response bias (Straub, Gefen, et al., 2005). Potential problems that could have resulted from challenges in using the Qualtrics research suite were not anticipated. This is because the researcher assumed that any person using a laptop or a desktop computer or any mobile device to perform her/his everyday duties would have the necessary competencies to enable him/her to participate in the study effectively. For instance, he or she must have a corporate email address; he or she would be able to follow simple instructions in order to access the web-link containing the measurement items and he or she is

knowledgeable enough on the topic to give appropriate and reasonable responses (Klassen & Jacobs, 2001). However, some scholars emphasise the value of collecting a second data set by using a paper based survey to guarantee non-respondent bias (Boyer, Olson, Calantone, & Jackson, 2002; Klassen & Jacobs, 2001; Simsek & Veiga, 2000). This approach was deemed unnecessary because it was assumed all potential respondents would be capable of responding to the web-based survey.

By and large, the survey approach reflected many of the benefits drawn from quantitative research. For instance, (a) the survey was useful in investigating the association between variables (Straub, Gefen, et al., 2005), (b) it was cheaper to administer. Moreover, (c) the cost per respondent was reduced dramatically and (d) less time was needed in processing the survey responses due to the reduced number of potential mistakes from interpretation of the respondent's handwriting and e-mail follow-ups (Simsek & Veiga, 2000).

3.4.2 Instrument Validation

Instrument validation required the evaluation of content validity, construct validity and reliability (Chang & King, 2005; Rivard et al., 2006; Straub et al., 2000). A validated measuring instrument provided for a consistent evaluation mechanism that allowed comparisons, differences or replication across end-users and groups (Baroudi & Orlikowski, 1988; Scott, 1995; Straub, 1989). Instrument validation was necessary for a number of reasons: (1) it facilitated the establishment of a cumulative research tradition, (2) it provided for enhanced measurement of research variables, (3) it helped in improving the clarity of research questions, and (4) it led to more meaningful variable relationships (Baroudi & Orlikowski, 1988; Straub, 1989). The use of an un-validated instrument had the potential to cause uncertainty in interpreting research findings, and offers no protection against the effects of confusing variables (Straub, 1989).

Content validity is a qualitative evaluation of the degree to which the measures of a construct actually capture its real nature. In general, content validity of an instrument is established through a pre-test which helps to get rid of measurement errors caused by poorly worded or ambiguous questions or instructions. Pre-testing of the instrument was necessary to ensure that all questions are appropriate and understood (Lewis, Templeton, & Byrd, 2005). Pre-testing for the survey instrument used in this research was achieved by running a pilot test that involved a total of 15 end-users from different organisations (participating organisations

not included). These people were approached to seek their opinions about the survey instrument. The feedback indicated that the concept of crisis preparedness in the context of the Information Systems was clearly understandable to the wider audience. Nevertheless, some comments and suggestions were made by the participants and they were incorporated into the final survey tool. In other words, content validity assured for the theoretical meaningfulness of a concept (Bagozzi, 1980) and the logic behind the data analysis (Pedhazur & Schmelkin, 1991).

Construct validity reflects the extent to which a given test is an effective measure of a theoretical construct (Straub et al., 2000). In simple words, the purpose of construct validity is to validate the theory behind the construct (Pedhazur & Schmelkin, 1991). However, since this study is not developing theory it was considered unnecessary to undergo comprehensive tests of construct validity (Boudreau et al., 2004). This is because in descriptive studies the testing of strength of relationships between constructs is not required. As indicated earlier in *Section 3.4*, this study only established facts based on the sample data and testing of the research hypotheses.

Reliability analysed the extent to which measurements are repeatable (Straub, 1989; Boudreau, Gefen, & Straub, 2004). In other words, reliability reflects the extent to which the measurements can provide consistent measures over time and across different studies (Nelson, Lurie, & Wasserman, 2007). Reliability was assessed by using the Cronbach's alpha (α) technique (Scott, 1995). As such, validation of the instrument only considered content validity and the reliability tests.

3.5 Operationalisation of CPIS Measures

The developed survey tool (appendix B) measured: (a) end-user knowledge and understanding of different aspects of the crisis preparedness of the information systems based on the available information from a range of societal legislative requirements such as information security incident management system standards (ISO/IEC 27035:2011), crisis management— guidance and good practice (PAS 200:2011), business continuity management (SAA/SNZ HB 221:2004), trade sector standards, including the organisational IS regulations, policies and procedures, (b) attitude towards CPIS, (c) normative expectations about peers, superiors and colleagues in the work place, (d) intention to comply with CPIS measures, (e) perceived vulnerability to IS risks and threats, (f) perceived seriousness of

crisis events outcomes, (g) response efficacy to offset potential threats, (h) self efficacy to cope in crisis situations, and (i) awareness of different aspects of the crisis preparedness of the information systems. These measures reflect attitude, normative belief and intention constructs of the TRA including the cognitive processes construct of the PMT. The cognitive processes construct embraces two major processes: threat appraisal and coping appraisal.

On the basis of the TRA and the PMT theoretical frameworks six variables out of seven were devised for this study: attitude towards CPIS, normative expectations, intention to comply, threat appraisal, response efficacy, and self efficacy. These variables were measured by scales developed and validated in prior research studies on cross-cultural dimension of technology use, security of wireless networks and human behaviour towards computer and information systems security. The seventh variable, crisis preparedness awareness was measured by a scale developed as part of this study. Since none of these measures were previously tested in the context of crisis preparedness of the information systems, the current study tests these measures in that context. Table 3.1 presents the research variables and their definitions, including the number of items per variable and the original scale source.

Table 3.1: Research Variables with their Respective Definitions

Variable	Variable Definition	Number of items	Source of the original scale
Attitude towards CPIS	The degree to which an end-user values different aspects of the crisis preparedness of the information systems	5	Pahnila, Siponen and Mahmood (2007b)
Normative expectations	The extent to which an end-user believes that peers, superiors and colleagues in the work place think or expect that he/she should either abide or not abide by CPIS measures	4	Lippert and Volkmar (2007)
Intention to comply	The extent to which an end-user is likely to perform the established measures of the crisis preparedness of the information systems	6	Siponen, Pahnila and Mahmood (2007)
Threat appraisal	The extent to which an end-user believes that he/she is truly confronted by IS risk and/or threat and that if nothing is done about it, it can develop negative consequences	4	Woon et al., (2005)
Response efficacy	The degree to which an end-user believes that his/her coping action will offset a potential threat	7	Pahnila et al., (2007a), Pahnila et al., (2007b)
Self efficacy	The degree to which an end-user believes that his/her ability or judgement will enable him or her to cope in a crisis situation	7	Siponen et al., (2007)
Crisis preparedness awareness	The extent to which end-users' knowledge and understanding of different aspects of CPIS in their organisation is fundamental for them to effectively execute CPIS measures.	8	Yuan and Jang (2008)

A brief discussion on each variable follows below. The specific text for all scale items can be found in *appendix C*.

Attitude towards CPIS is defined as the degree to which an end-user values different aspects of the crisis preparedness of the information systems within the organisation. Attitude indicates an end-user's positive or negative beliefs towards CPIS measures. Attitude towards CPIS was measured by the end-user's responses to five items requesting them to indicate to what degree they perceived their contribution is important to the effectiveness of the CPIS measures. The attitude towards CPIS variables is adapted from the scale used by Pahnila, Siponen and Mahmood (2007b) when they measured attitude towards IS security compliance.

Normative expectations is defined as the extent to which an end-user believes that peers, superiors and colleagues in the work place think or expect that he/she should either abide or not abide by CPIS measures. This variable was measured by asking the respondents to rate their behaviour as a result of the influence resulting from interactions in their work place community. Their responses were based on four items. The variable "normative expectations" has its origin in TRA (Ajzen & Fishbein, 1980), but it has also been used by Lippert and Volkmar (2007) to measure cultural effects on technology in an organisation setting.

Intention to comply refers to the extent to which an end-user is likely to perform the actions as stipulated in the measures of the crisis preparedness of the information systems. This variable signifies end-users' willingness to attempt to perform the behaviour in question (Ajzen, 1991) — compliance with CPIS. End-users' intentions were measured by requesting the respondents to indicate their willingness to perform or not to perform a range of behaviours expected of them. This involved responding to six items on a seven-item scale. The intention to comply which is based on TRA (Fishbein & Ajzen, 1975) has also been used by Siponen, Pahnila and Mahmood (2007) to measure employees' adherence to security policies.

Threat appraisal is defined as the extent to which an end-user believes that he/she is truly confronted by the IS risk and/or threat and that if nothing is done about it, it can develop into a negative consequence. This variable was measured by asking the respondents to indicate their perceptions on whether their organisation is vulnerable to IS risks and threats, which may take place if nothing is done to offset them and if they thought there was any potential

harm to the organisation that could result from those events. This involved responding to four items of the survey instrument. Threat appraisal which is based on PMT (Maddux & Rogers, 1983) has also been used by Woon et al., (2005) to measure home users' decisions on whether or not to use security features.

Response efficacy measures the degree to which an end-user believes that his/her coping action will offset a potential threat. This variable was measured by asking respondents to rate their beliefs in the perceived benefits of their coping actions (Rogers, 1975)— the CPIS measures and their beliefs that performing the coping action will actually offset the threat. End-users were required to respond to seven items on a five-item scale. Similar to threat appraisal, response efficacy is also based on PMT (Maddux & Rogers, 1983). The variable has been used in several studies. For instance, Pahnila et al., (2007a) used the response efficacy variable to identify factors that explains employees' adherence to information security policies. In addition, Pahnila et al., (2007b) used the same variable to understand employees' behaviour towards IS security policy compliance.

Self efficacy measures the degree to which an end-user believes that his/her ability or judgement will enable him or her to cope in a crisis situation. This variable attempted to capture the perceived capability (Woon et al., 2005) to make use of various CPIS measures. In other words, it tests the belief in one's own ability to do something (Bandura, 1977), in this context, carrying out CPIS measures. End-users were required to respond to seven items on the survey instrument. Self efficacy which is based on PMT (Maddux & Rogers, 1983) has also been used by Siponen et al., (2007) to investigate employees' adherence to information security policies.

Crisis preparedness awareness measures the extent to which end-users' knowledge and understanding of different aspects of CPIS in their organisation is fundamental for them to effectively execute CPIS measures. This variable attempted to capture the positive influence that can be presented by an understanding of the broader picture of crisis preparedness in terms of relationships between stakeholders, information sharing, activities, processes and procedures (Al-Zarouni, 2006; Tetmeyer & Saiedian, 2010). End-users were required to respond to eight items on the survey instrument. The crisis preparedness awareness variable draws on marketing concepts which use awareness measures to check marketing and advertising effectiveness (Romaniuk, Sharp, Paech, & Driesener, 2004). This is because

when a person becomes familiar with a brand through repeated exposure, his/her perceived risk tends to decline and positive affect tends to increase (Yuan & Jang, 2008). Hence, the wine/winery awareness variable from a wine festival model is reworded accordingly to fit this study.

3.6 Ethical Considerations

Approval was obtained from the School of Information Management Human Ethics Committee. The researcher also ensured that the requirements of the New Zealand *Privacy Act 1993* that sets out principles for the collection, use, disclosure, security and access to personal information were met before starting the survey. The ethical requirements were presented in the information sheet (*Appendix A*) for the participants to consult prior to any engagement in the research. All data collected were kept confidential. No other person apart from me and my supervisor, Dr. Philip Calvert, saw the survey responses and we were not able to identify who they came from. All survey responses were kept in a password protected file on a secure server and formed the basis of my research, but only aggregated data has been used to write this report. The survey responses will be destroyed two years after the end of the project.

3.7 Chapter Summary

In this chapter an outline of the design for the empirical research was provided. It starts with the research paradigm, the ontological approach which is realism, with a positivist philosophy. The methodological approach uses quantitative methods. This is followed by a detailed description of the quantitative methods. An indication was provided of how the actual data collection and analysis fitted into the research design. Finally, the ethical considerations that guided this study were presented.

Chapter 4: Data Analysis and Results

4.1 Introduction

The literature identifies diverse methods for analysing quantitative data. Predominantly, these methods make use of statistical tools and packages to carry out the required data analysis. For the purposes of effectiveness, statistical tools and techniques use numbers to represent values and levels of theoretical constructs and concepts.

This chapter presents the data analysis and the results of the study. First, information about the survey respondents is provided. This is followed by the data preparation process, the response rate and the respondents' demographics. Thereafter, reliability tests and descriptive statistics are presented followed by the correlation analyses. Finally, a concise summary of the chapter is provided.

4.2 About the Survey Respondents

Potential respondents came from a set of 16 organisations which operate across New Zealand. These were from the following sectors: Energy, Service industries, Telecommunication, Tertiary Education, Banking and Information Systems (or IT).

Initial communication to the respondents to request their input into the study was done either by phone or email. The email introduced the researcher to the respondents' organisations as well as the general view of the subject of the research. Both email and phone communications were followed by a second communication which was an email containing two key documents (i.e. a brief research proposal and a survey tool). These two documents were used by the management of the respondents' organisations to decide whether to allow or to decline the study request to collect data from end-users of the information systems in those organisations.

Among the 16 organisations that were approached to participate into the study, only 3 organisations agreed to my study request. This was a dramatic 81% reduction from the original pool of 16 possible respondent organisations (See Table 4.1). Many of these organisations simply indicated that they were unable to participate due to demanding

workload and time constraints. However, they indicated that they could participate in similar studies in the near future.

Table 4.1: Organisations Statistics

Number of organisations **approached**	Number of organisations that **accepted**	Number of organisations that **declined**
16	3	13
100%	18.75%	81.25%

The three organisations that accepted my study request came from three different sectors. Organisation A is an energy company that had just gone through a year long process of raising staff awareness of crisis preparedness of the information systems. Organisation B is a service company that provides a range of communication and business solutions throughout New Zealand. There was no indication of any awareness activities associated with crisis preparedness of the information systems in recent past. Organisation C is a tertiary institution, providing higher education to people from all nationalities and from all walks of life. In this institution, awareness activities with regard to crisis preparedness of the information systems are usually reserved for key people that are directly involved into crisis preparedness strategies. All three organisations have more than 100 employees; hence they fit into Statistics New Zealand's definition of large companies.

4.3 Data Preparations

This study used a self reporting perception survey to capture information systems end-users' responses to seven dimensions: Attitude towards CPIS, Normative expectations, Intention to comply, Threat appraisal, Response efficacy, Self efficacy, and Crisis preparedness awareness. Once the set duration for the data collection exercise had expired, end-users' responses were checked for completeness. The data collection duration comprised of two consecutive three weeks sessions— i.e. six weeks in total. Checking for completeness ensured that the data was clean and error-free. Thereafter, data was entered into SPSS 19.0.

Fundamentally, the data preparation process concentrated on the survey questions which were likely to produce missing data. This included questions which could have produced a response of (1) none of the above, (2) I don't know, or (3) a blank space. A "None of the

above" response was coded 11 while "I don't know" and "blank space" responses were coded 9 and dot (.) respectively.

Table 4.2: Summary of Missing Responses

	Item— List other activities that embraces CPIS	**Percentage %**
Number of responses— Missing	44	61.1%
Number of responses	28	38.9%
Total number of respondents	72	100%

There were generally a minimal number of responses missing. However, as Table 4.2 indicates, Item S2.2 – 'List other activities that embraces CPIS' – was responded to by only 28 respondents out of 72, which is about 39% of the total responses to that particular item. The fewer number of responses to this question could be because there were no other CPIS activities that existed in those organisations or end-users were completely unaware of crisis preparedness initiatives in their organisations. For other items, the completeness of data was facilitated by a feature in the Qualtrics application that forced the participants to respond to each pending question before proceeding to a subsequent question.

Data preparation also involved coding multiple response items (*Appendix D*). These are the questions that required the respondents to provide more than one response. Since it is impossible to record these items as a single variable into the SPSS application, it was necessary to create as many component variables as there were items in the list. Each recorded response was labelled "Yes" and coded with a value of 1. And all non-recorded responses were discarded.

18 responses were excluded from the dataset prior to the data analysis. These were incomplete responses that were started but never completed by their authors. They only contained demographic information. In total, 72 responses of the 90 web-surveys received were identified for data analysis procedures.

4.4 Response Rate

In total 297 email invitations were sent out to potential participants (see Table 4.3). In average 10 minutes were spent by the majority of the respondents to complete the survey. The response rate to the survey was 30%. This is well below the 60% mark which is considered to be "good" for statistical accuracy (Sivo, Saunders, Chang, & Jiang, 2006). Despite every effort to uplift the response rate, 30 percent was the final yield. Some of the efforts included running the pilot test, incorporating the suggested changes (about the design and the instrument questions) to improve the respondents' experience, and sending out two reminders.

Table 4.3: Expected Responses versus Actual Responses

	Expected response rate	Actual response rate
Survey sample size	297	297
Response rate	60%	30%
Participant responses	178.2	90

Nevertheless, the 30% response rate is still considered to be reasonable for organisational surveys. This is because a 30% response is slightly higher than many of the reported response rates in published IS research studies which considered response rates in the 17%- 28% range to be reasonable (Jarvenpaa & Staples, 2001; Ravichandran & Rai, 2000).

The Web-based survey was voluntary and the respondents were identified from a group of employees with help from the participating organisations. The web-based survey was comprised of forty closed questions and one open question. Potential respondents were required to read an information sheet prior to their engagement into the study. Based on the information provided in the information sheet respondents were at liberty to indicate their willingness to participate into the study by either choosing to "agree" or to "disagree". Respondents who agreed to participate into the study were required to respond to all questions to successfully complete the survey.

There are many factors that could have contributed to the low response rate. These may include (1) unwillingness to respond to an unsolicited survey, (2) lack of motivation to

complete the survey as no incentives were promised in return, and (3) a shortage of time to start and ultimately complete the survey (Bryman, 2008).

In future studies low responses could be overcome by requesting the top management team to take on the research project as their own. In this way they can promote it to their employees. In addition, some kinds of motivation in terms of prizes or supermarket vouchers can be promised in return for research assistance.

4.5 Demographics

Figures 2.7 and 2.8 present the distribution of respondents in terms of the years worked in the current organisation and the age group. Table 4.4 indicates that the majority of the respondents (53%) have worked in their current organisation between 1 to 10 years. This is an indication that the respondents have spent enough time with their respective organisations to comment on different processes, procedures and strategies with regard to CPIS.

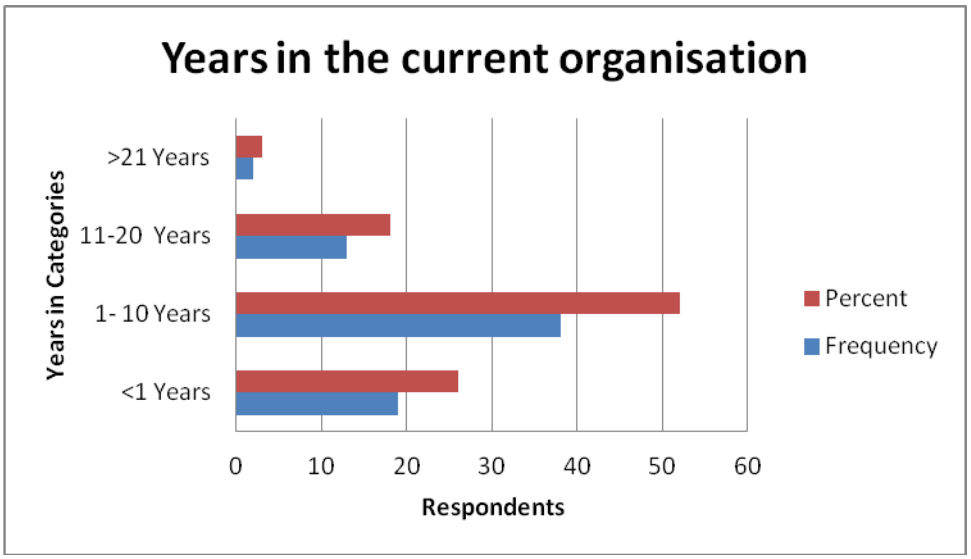

Figure 2.7: Years with the Current Organisation

From a different perspective, 56% of the respondents fall into the (31-45) age group. This could possibly indicate that the respondent were mature enough to provide invaluable information to which the degree of crisis preparedness of the information systems could be measured.

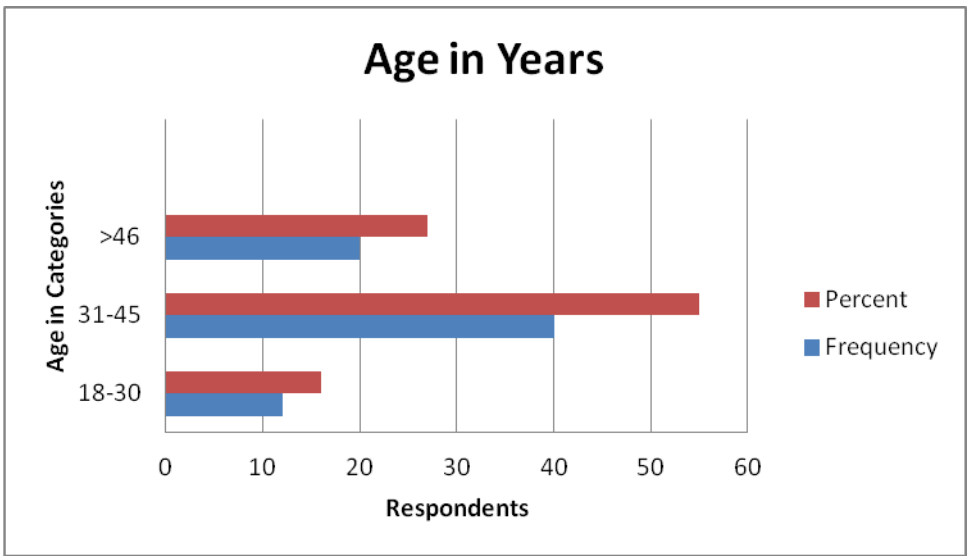

Figure 2.8: Age in Years

Table 4.4 demonstrates key attributes of the respondents. From the respondents' demographics it could be assumed that the sample was well distributed and that the respondents were reasonably qualified to participate in the study.

Table 4.4: Demographics

Measure	Items	Frequency	Percent
Gender			
	Male	51	70.8%
	Female	21	29.2%
Age			
	18-30	12	16.7%
	31-45	40	55.6%
	>45	20	27.8%
Role			
	IT/IS	54	75.0%
[Your department]	Other	18	25.0%
EMP	<1	19	26.4%
	1-10	38	52.8%
[Years with the current organisation]	11-20	13	18.1%
	>20	2	2.8%

Their eligibility was based on their knowledge about the information systems and their familiarity with different CPIS strategies that their organisations could utilize to counteract crisis events that could negatively affect the information systems platforms.

4.6 Reliability Tests

The reliability indices were calculated by SPSS 19 using Cronbach's alpha procedure (Gray & Kinnear, 2011). As shown in Table 4.5, Cronbach's α for the variables range from 0.417 to 0.863; as such a high internal consistency cannot be claimed. Nunnally and Bernstein (1994) suggest that a value for Cronbach's α greater than 0.70 indicates a satisfactory level of item reliability. In this particular study, only two variables (see section 3.5) were considerably above this threshold and one variable came close to it.

Table 4.5: Reliability Coefficients

Variable	Cronbach's Alpha (α)
Attitude Toward CPIS	**0.560**
Normative Expectations	**0.863**
Intention to Comply	**0.692**
Threat Appraisal	**0.504**
Response Efficacy	**0.761**
Self Efficacy	**0.417**
Crisis Preparedness Awareness	**0.461**

However, the minimal standard α value which is 0.7 has been met only by two constructs: normative expectations and response efficacy. In that sense, these alpha values: 0.417, 0.461, 0.504 and 0.560 were considered to be moderately good. Therefore, the questionnaire tool used for this study provided an adequate level of reliability for hypothesised measures of the variables (Boudreau et al., 2004).

4.7 Descriptive Statistics

In order for this report to be understood by a wider audience, it was important to replace the SPSS variables (e.g. CPA1.1, ATTC1) with abbreviated forms of the original questions. With this change in place it becomes much easier for the reader to link the displayed data to the actual variable being studied. Table 4.6 presents different names of the study variables as they were used for data analysis in this study.

Table 4.6: The Variables with their Respective Abbreviated Questions

Item	SPSS Variable	SPSS Label	*Abbreviated questions*
		Demographics	
D1	**Gender**	Gender	**Gender**
D2	**Age**	Age in Years	**Age in Years**
D3	**Role**	Your department	**Your department**
D4	**Employ**	Years in current organisation	**EMP**
		Crisis Preparedness Awareness	
S2.1.1	**CPA1.1**	Does establishment of plans represent crisis preparedness?	**Establishment of CP plans**
S2.1.2	**CPA1.2**	Does continuous managing of risks and threats represent crisis preparedness?	**Continuous management of risks**
S2.1.3	**CPA1.3**	Do identification, control and mitigation of security measures embrace crisis preparedness efforts?	**Identification, control and mitigation**
S2.1.4	**CPA1.4**	Do plans and procedures to facilitate restoration of affected systems represent crisis preparedness?	**Procedures to facilitate restoration**
S2.1.5	**CPA1.5**	Do end-users sharing information about security represent crisis preparedness?	**Sharing security information**
S2.1.5	**CPA3**	CPIS responsibility in my organisation lies with...	**Responsibility lies with**
S2.1.5	**CPA5.1**	Unauthorised internal system access	**Unauthorised internal access**
S2.1.5	**CPA5.2**	Unauthorised external system access	**Unauthorised external access**
S2.1.5	**CPA5.3**	Unexpected system shutdown	**Unexpected shutdown**
S2.1.5	**CPA5.4**	Natural disasters (e.g. Floods, Earthquakes)	**Natural disasters**
S2.1.5	**CPA5.5**	Fire breakout	**Fire breakout**
S2.1.5	**CPA5.6**	Non-compliance with organisational information security policies	**Non-compliance**
S2.1.5	**CPA5.7**	Some of the incidents that are capable of causing significant damages to the IS ...-None of the above	**Deleted (**Zero response**)**
S2.1.5	**CPA5.8**	Some of the incidents that are capable of causing significant damages to the IS...-I don't know	**Deleted (**Zero response**)**
S2.1.5	**CPA6**	Are you aware of any period(s) that the information systems of your organisation went through a crisis?	**Awareness of past crisis event?**
S2.1.5	**CPA7**	CP measures are processes that allow the organisation to function in times of uncertainty	**CP measures allow performance even in uncertainty**
S2.1.5	**CPA8**	In my organisation crisis preparedness processes and procedures are kept current	**CP Measures are kept current**
		Attitude Towards CPIS	
S3.3	**ATTC1**	CPIS is mainly the responsibility of all employees within the organisation	**Responsibility of all employees**
S3.4	**ATTC2**	CPIS is not an independent activity rather it is incorporated into day to day activities	**CP is incorporated into day to day activities**
S3.5	**ATTC3**	CPIS is an activity that I must perform separately to my daily duties	**CP performed separately to daily duties**
S5.6	**ATTC4**	Do you think the implementation of the measures for CPIS requires full participation of end-users?	**Participation of all users**
S3.1	**ATTC5**	CPIS is primarily the responsibility of a selected group of people	**Responsibility of a selected group of people**
		Normative Expectations	
S5.7	**NE1**	The implementation of crisis preparedness measures requires all teams (e.g. Information Technology/I...	**Requires all teams participation**
S5.8	**NE2**	In the implementation of the measures for CPIS, collaboration is not necessary	**Collaboration is not necessary**
S7.8	**NE3**	Cp training and communication provide for employees to know their roles in the event of a crisis	**Training provide the know how in crisis events**
S7.9	**NE4**	Cp training and communication has created a readiness for end-users to work together	**Training allows working together**

		Intention to Comply	
S4.5	**ITC1**	In the occurrence of a major disastrous event such as an earthquake, fire breakout or flooding, what...	**What will be your first reaction?**
S9.1.1	**ITC2**	A requirement that you change your security password every 60 days	**Change your password regularly**
S9.1.2	**ITC3**	Your new security password must be eight characters long and must combine letters, symbols and figures	**Ensure strong password**
S9.1.3	**ITC4**	The system logs you off when you are idle for five minutes either working from your office or remotely	**Strict information access control**
S9.2.1	**ITC5**	Ensure complete back up of all personal generated information at the end of every week	**Ensure regular back up of data**
S9.2.2	**ITC6**	Conduct a trial run to retrieve backed up information after every six months	**Conduct regular trial runs**
		Threat Appraisal	
S4.1	**TA1**	It is probable that my organisation will encounter some of the threats and risks common to information systems	**My organisation is likely to be affected**
S8.1	**TA2**	Failure by end users to perform correct measures will lead to negative consequences	**Lack of adherence lead to negative consequences**
S8.2	**TA3**	I think unexpected system shutdown as a result of non compliance is a serious issue for the org...	**Non compliance is a serious issue**
S4.4	**TA4**	Do you think the allowance to BRING YOUR OWN DEVICE to work has any detrimental effects	**Personal devices at work have detrimental effects**
		Self Efficacy	
S4.2	**SE1**	Information about potential crises have been communicated to all stakeholders	**Information has been communicated to all**
S5.5	**SE2**	Measures for CPIS in my organisation are developed enough to cope in crisis situation	**CPIS measures can cope in a crisis situation**
S6.2	**SE3**	I believe measures for the CPIS in my organisation have been operationalised	**CPIS measures are operational**
S6.4	**SE4**	In my organisation crisis preparedness processes and procedures are reviewed every	**Measures are reviewed**
S7.1	**SE5**	Crisis preparedness training is conducted in the following intervals.	**Fixed training schedules**
S7.3	**SE6**	Cp training is conducted when a new crisis preparedness measure is being implemented	**Training when there is a change**
S7.6	**SE7**	My crisis preparedness training are in-line with assigned duties and tested responsibilities	**Training is in-line with my duties**
		Response Efficacy	
S5.2	**RE1**	If Yes, do you believe that crisis preparedness measures in your organisation have improved from the...	**Improvement has been done**
S5.3	**RE2**	How would you rate the level of CPIS of your organisation as compared to others in the sector.	**Your organisation in comparison to others**
S5.4	**RE3**	CPIS measures will protect critical business processes from potential IS threats and risks	**Critical systems will be protected**
S7.2	**RE4**	Crisis preparedness training is conducted during the induction (orientation) programme	**Training during induction**
S7.4	**RE5**	I cannot recall any crisis preparedness training being conducted in my organisation	**No training at all**
S7.5	**RE6**	My Cp training involves crises simulation so that I know exactly what to do in times of crises...	**Training involves simulation**
S7.7	**RE7**	My Cp training include introduction to available resources and tools to use in the event of a crisis	**Resources and tools are available**

In this study, descriptive statistics calculated the mean, the range, the standard deviation, the minimum and the maximum values for each variable. Responses to at least four variables were consolidated to describe the main variable based on the collected data. Different tables and figures that describe the seven main variables are displayed next.

Attitude Towards CPIS

Descriptive statistics for end-users' attitudes toward the crisis preparedness of the information systems are reported in Table 4.7 and Figure 2.9.

Table 4.7: Descriptive Statistics - Attitude Towards CPIS

	N	Range	Mini	Maxi	Mean	Std. Deviation
CP is the responsibility of a selected group of people	70	4	1	5	3.27	1.17
CP is the responsibility of all employees	70	4	1	5	2.77	1.12
CP is incorporated into day to day activities	67	4	1	5	3.33	1.02
CP performed separately to daily duties	67	4	1	5	2.70	.99
CP requires participation of all users	61	4	1	5	3.08	1.27
Valid N (listwise)	61					

All five variables were measured on a five-item scale, 1-strongly disagree and 5-strongly agree. Hence the middle value is 3. Most of these variables have mean responses close to 3, a minimum of 1 and maximum of 5. The range stands at 4. All variables have a standard deviation greater than 1 except one (ATTC3) which has a S.D of .99. Variables with higher standard deviations indicated a reasonable degree of variability in the data.

The high mean response of 3.27 indicates that many of the respondents believe that the responsibility for the crisis preparedness of the information systems belongs to a selected group of people (ATTC5). This is also evident in the percentage of responses which shows that 55.7 percent of respondents agree that the responsibility for CPIS should be handled by a selected group of people.

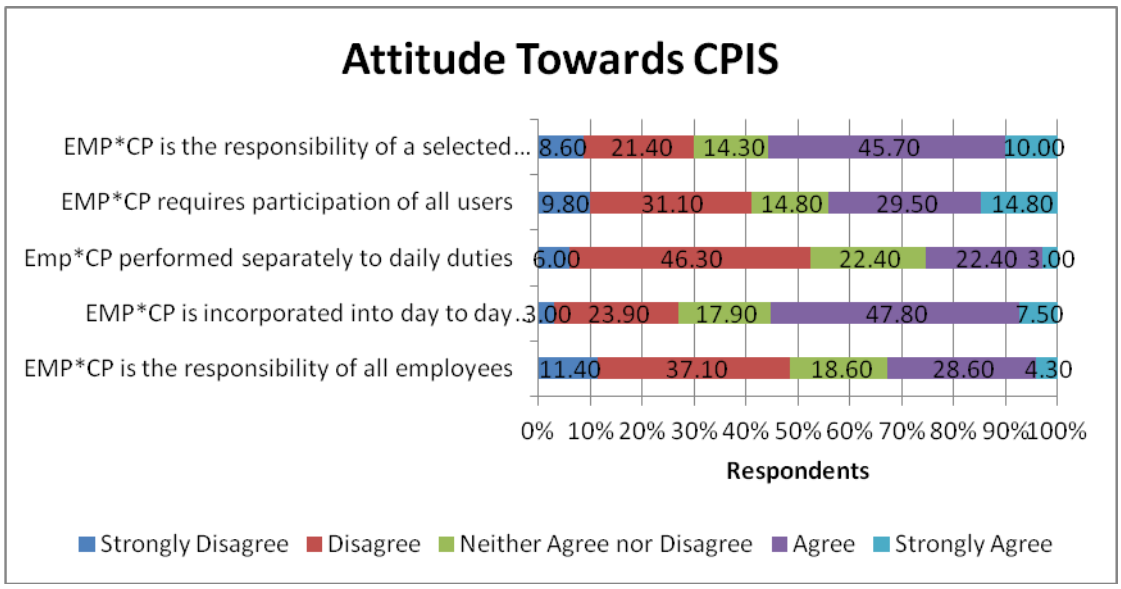

Figure 2.9: Attitude Towards CPIS - Statistics

Nevertheless, a high mean response of 3.33 indicates that most respondents believe that CPIS initiatives should be incorporated into day to day activities (ATTC2). A sizeable 55.3 percent of respondents agreed to this opinion and 52.3 percent disagreed to the statement that CP duties be performed separately to daily duties (ATTC3).

Normative Expectations (NE)

Descriptive statistics for end-users' normative expectations about the crisis preparedness of the information systems are reported in Table 4.8 and Figure 2.10. All four variables were measured on a five-item scale. Hence the middle value is 3. One variable has a mean close to 4. Two variables have mean responses close to 3 and one variable has a mean close to 2. Minimum values range from 1 to 2 and maximum values range from 4 to 5. Range values stand at 3 and 4.

Table 4.8: Descriptive Statistics - Normative Expectations

	N	Range	Mini	Maxi	Mean	Std. Deviation
Requires all teams participation	61	4	1	5	3.95	.99
Collaboration is not necessary	61	3	1	4	1.90	.91
Training provide the know how in crisis events	53	3	2	5	3.17	.91
Training allows working together	53	3	2	5	3.17	.87
Valid N (listwise)	53					

Most respondents agree that crisis preparedness initiatives require the participation of teams such as Information Technology, Business units and Human Resources (NE1). This is indicated by the high mean response of 3.95. No less than 74 percent of respondents agreed to that proposition (see Fig. 2.10).

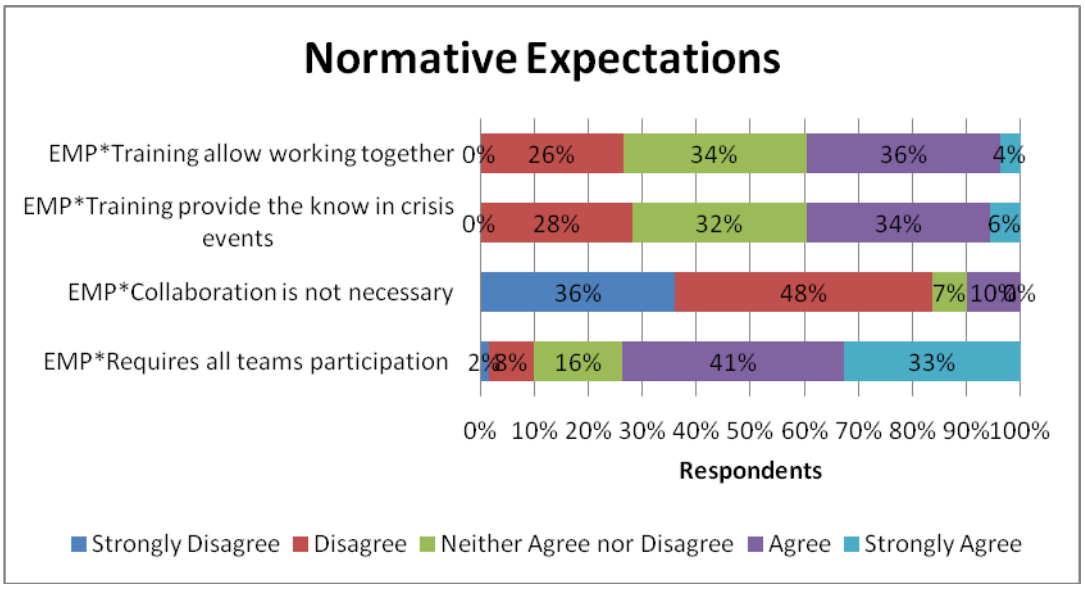

Figure 2.10: Normative Expectations - Statistics

The same question when asked in a reverse order produced a low mean response of 1.90. This indicates that end-users believe that collaboration in CPIS endeavours is necessary. This is also evident from a sizeable 84 percent of respondents who disagreed with the statement that "collaboration is not necessary" (NE2).

Intention to Comply (ITC)

Descriptive statistics for end-users' intention to comply with measures for crisis preparedness of the information systems are reported in Table 4.9, Figures 2.11 and 2.12.

Table 4.9: Descriptive Statistics - Intention to Comply

	N	Range	Mini	Maxi	Mean	Std. Deviation
What will be your first reaction?	62	2	1	3	2.66	.68
Change your password regularly	59	6	1	7	3.61	1.70
Ensure strong password	59	6	1	7	4.76	1.32
Strict information access control	59	6	1	7	2.98	1.88
Ensure regular back up of data	59	5	2	7	5.07	1.27
Conduct regular trial runs	59	5	2	7	5.29	1.13
Valid N (listwise)	59					

Five variables were measured on a seven-item scale, 1-very displeased and 7-very pleased. One variable (ITC1) was measured on a five-item scale. Three variables out of five which were measured on a seven-item scale have mean responses above 4, which are 4.76, 5.02 and 5.29. Minimum values range from 1 to 2 and maximum values range from 3 to 7. Range values stand at 2, 5 and 6. All variables have a standard deviation greater than 1 except one (ITC1) which has a S.D of .68. Higher standard deviations indicate a moderate degree of variability in the data.

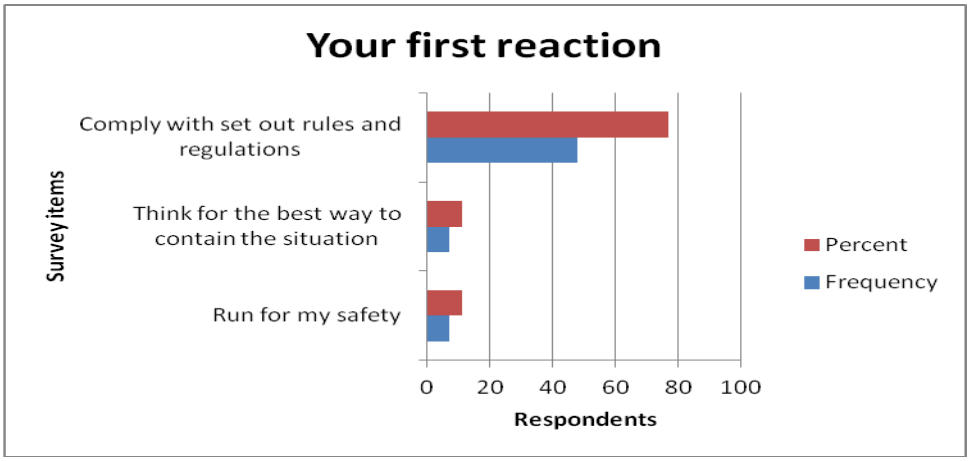

Figure 2.11: Your First Reaction during a Crisis Event

On the question "what will be your first reaction?" (ITC1) most respondents indicated their intention to comply with the set out rules and regulations. This is clear from the high mean response of 2.66 on a five-item scale. No less than 77 percent of respondents indicated their intention to comply with rules and regulations that embrace crisis preparedness of the information systems (see Fig. 2.11).

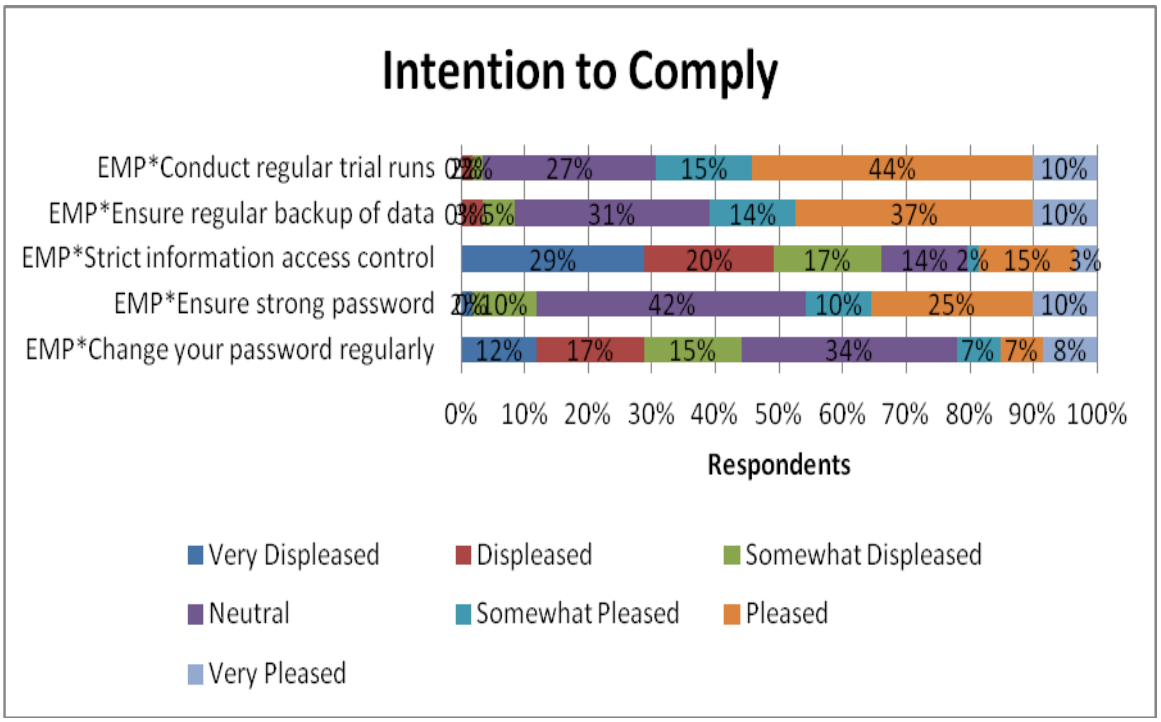

Figure 2.12: Intention to Comply - Statistics

Many respondents are pleased to conduct regular trial runs to recover their data. This is shown by a high mean response of 5.29 (see Table 4.9) and a considerable 54 percent of pleased respondents. Respondents are also pleased to regularly backup their data. This is clear from the high mean response of 5.07 and a reasonable 47 percent of pleased respondents. However, a substantial percentage of respondents seem to be neutral on the issues of secure passwords. While 42 percent of respondents had no opinion on ensuring strong passwords, 34 percent lacked an opinion on changing their passwords on regular basis.

Threat Appraisal (TA)

Descriptive statistics for end-users' threat appraisal with regard to crisis preparedness of the information systems are reported in Table 4.10 and Figure 2.13. Three variables were measured on a five-item scale and one variable (TA4) was measured on a scale with these responses: Yes, No and I don't know.

Table 4.10: Descriptive Statistics -Threat Appraisal

	N	Range	Mini	Maxi	Mean	Std. Deviation
My organisation is likely to be affected	62	4	1	5	2.77	1.02
Lack of adherence lead to negative consequences	59	3	2	5	3.53	.70
Non compliance is a serious issue	59	3	2	5	3.44	.93
Personal devices at work have detrimental effects	59	8	1	9	2.75	2.71
Valid N (listwise)	59					

Two variables out of three which were measured on a five-item scale have mean responses above 3. Minimum values range from 1 to 2 and maximum values range from 5 to 9. Range values stand at 3, 4 and 8. The variables TA1 and TA4 have standard deviations greater than 1 which shows some degree of variability in the data.

Many respondents believe that a lack of adherence to established CPIS measures can lead to negative impacts to the information systems of the organisation. This is evident from the high mean response of 3.53. This observation is also in-line with the high percentage of respondents (61%) who agreed that a lack of adherence to CPIS measures can lead to damages to the information systems of the organisation.

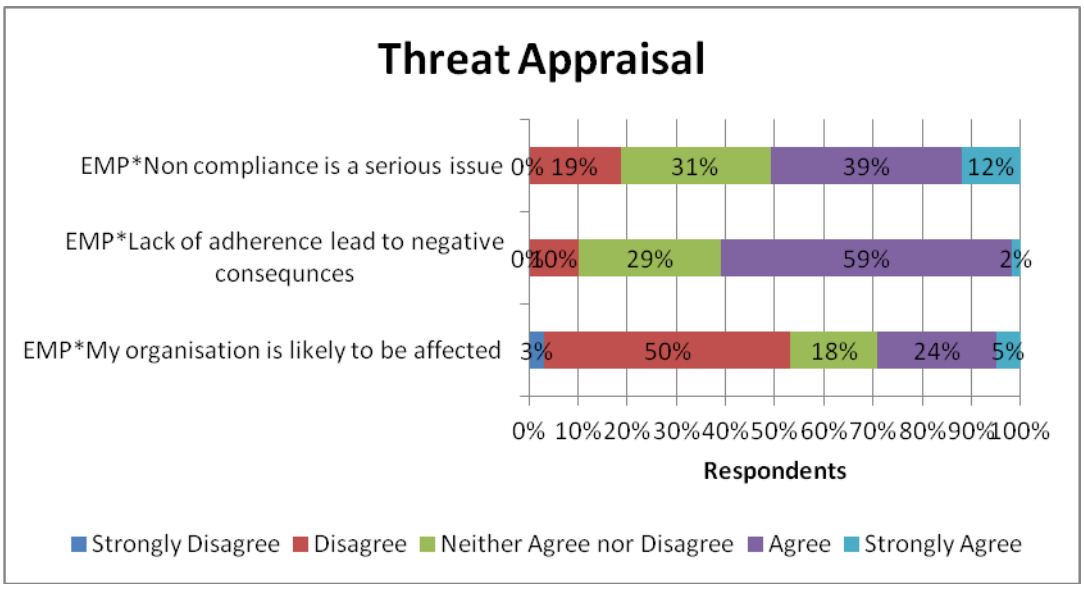

Figure 2.13: Threat Appraisal - Statistics

The high mean response of 3.44 for the TA3 variable reflects the perceptions of the respondents about the seriousness of non compliance. This means that many respondents perceive that CPIS non compliance is a serious matter from the organisation's perspective. This finding is consistent with a sizeable 51 percent of the respondents who agreed to the statement that "unexpected system shutdown as a result of non compliance is a serious issue for the organisation". On the contrary, 53 percent of respondents disagreed with the statement that their organisations are likely to encounter some of the threats and risks common to information systems.

Moreover, on the question which asked the respondents if they thought bringing their own devices (BYOD) to work had any detrimental effects to the CPIS of their organisation, the data indicate that many respondents are of the opinion that their devices are of no threat to the CPIS. This is indicated by the low mean response of 2.75 (see Table 4.10).

Response Efficacy (RE)

Descriptive statistics for end-users' response efficacy with regard to crisis preparedness of the information systems are reported in Table 4.11 and Figure 2.14. Five variables were measured on a five-item scale. The dimension (RE2) which requested the respondents to rate the CPIS of their organisation with those in the same sector was measured on a scale with Below Average, Average and Above Average responses. The other dimension (RE4), asked

the respondents to indicate if they received any formal training on CPIS during the induction period. This variable was measured on a scale with Yes and No responses.

Table 4.11: Descriptive Statistics - Response Efficacy

	N	Range	Mini	Maxi	Mean	Std. Deviation
Improvement has been done	44	3	2	5	4.00	.84
Your orgnisation in comparison to others	61	2	1	3	2.25	.70
Critical systems will be protected	61	3	2	5	3.66	.85
Training during induction	60	1	1	2	1.83	.38
No training at all	60	4	1	5	2.67	1.31
Training involves simulation	53	4	1	5	3.21	.99
Resources and tools are available	53	3	2	5	3.23	.82
Valid N (listwise)	39					

Four variables have mean responses above 3. Minimum values range from 1 to 2 and maximum values range from 2 to 5. Range values stand at 1, 2, 3, and 4. Many of the variables have a S.D of less than 1 except the RE5 variable which has a S.D greater than 1.

The high mean response of 4.00 indicates that many respondents have a feeling that the CPIS of their organisations has improved from the last known incident. This is consistent with a sizeable 79 percent of respondents who agreed that improvement has been made.

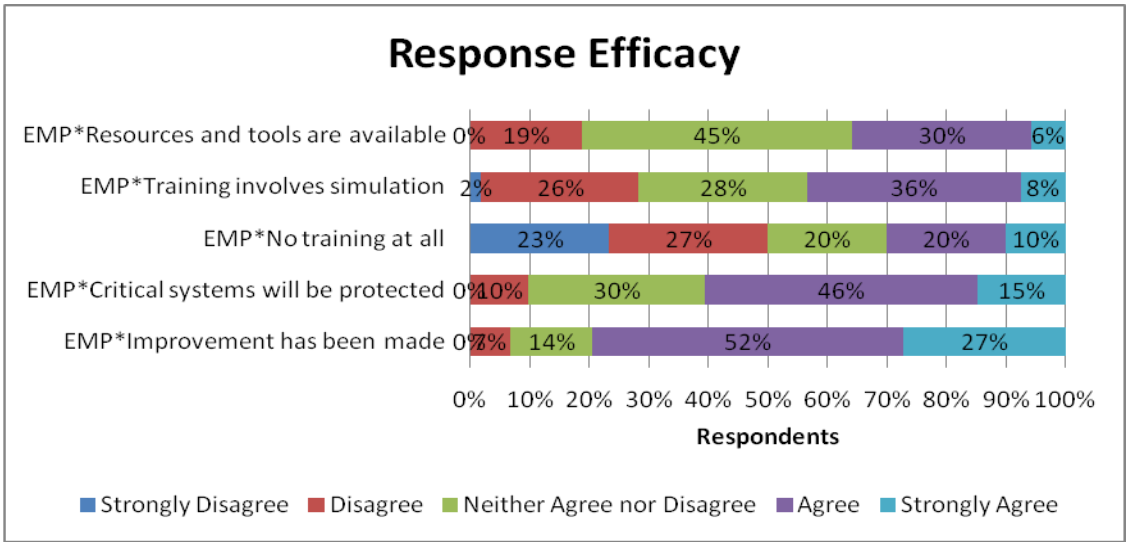

Figure 2.14: Response Efficacy - Statistics

On the other hand, many respondents believe that the implementation of CPIS measures will protect critical systems from IS threats and risks. This is evident from a high mean response of 3.66 and a huge 61 percent of respondents who agreed.

Nevertheless, a considerable 45% of respondents had no opinion if their CP training had introduced them to any resources and tools to use in the event of a crisis.

Self Efficacy (SE)

Descriptive statistics for end-users' self efficacy with regard to crisis preparedness of the information systems are reported in Table 4.12 and Figure 2.15. Five variables were measured on a five-item scale. Two dimensions (SE4) and (SE5) asked the respondents to indicate in terms of intervals when CPIS measures were reviewed, and after how long they were trained, respectively.

Table 4.12: Descriptive Statistics - Self Efficacy

	N	Range	Mini	Maxi	Mean	Std. Deviation
Information has been communicated to all	62	4	1	5	2.68	1.00
CPIS measures can cope in a crisis situation	61	3	2	5	3.54	.94
CPIS measures are operational	60	4	1	5	3.43	.87
Measures are reviewed	60	5	1	6	3.23	1.90
Fixed training schedules	60	10	1	11	6.42	4.95
Training when there is a change	60	3	2	5	3.03	.78
Training is inline with my duties	53	3	2	5	3.32	.78
Valid N (listwise)	53					

Minimum values range from 1 to 2 and maximum values range from 5 to 11. Range values stand at 3, 4, 5, and 10. The high mean response of 6.42 was for the item which requested the respondents to indicate the interval between CP trainings. Many of the respondents responded as "none of the above". Other options in that question included: once per year, after every two years, after every three years. This may indicate that there are no scheduled training programmes as far as CPIS is concerned, or possibly the provided categories did not match any of the established training schedules in those organisations.

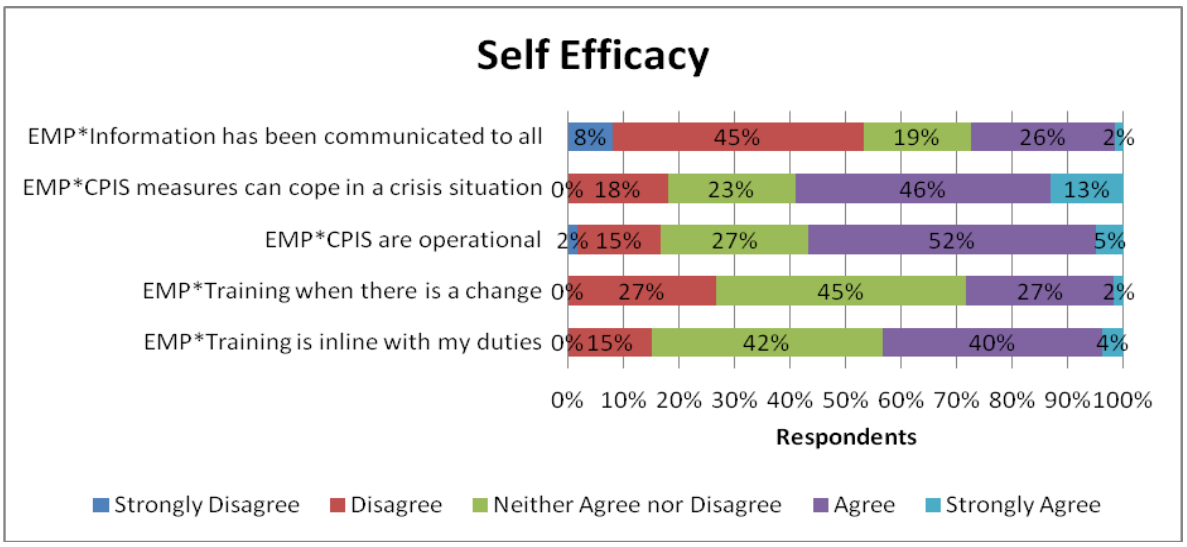

Figure 2.15: Self Efficacy - Statistics

This observation is also clear from the sizeable 45% and 42% of respondents who had no opinion on the two training dimensions: SE6 and SE7.

However, 46% and 52% of respondents had a feeling that CPIS measures have been operationalised (SE3) and can cope in crisis situations (SE2) respectively. This finding is also clear from the high mean responses of 3.43 and 3.54 for the similar variables.

Crisis preparedness awareness (CPA)

Descriptive statistics for end-users' crisis preparedness awareness of crisis preparedness of the information systems are reported in Table 4.13 and Figures 2.16 and 2.17.

Table 4.13: Descriptive Statistics - Crisis Preparedness Awareness

	N	Range	Mini	Maxi	Mean	Std. Deviation
CPIS responsibility in my organisation lies with...	70	8	1	9	3.23	1.64
Awareness of past crisis event?	62	1	1	2	1.27	.45
CP measures allow performance even in uncertainity	60	3	2	5	3.88	.83
CP Measures are kept current	60	3	2	5	3.43	.89
Valid N (listwise)	60					

The high mean response of 3.88 indicates that many respondents were aware that the existence of CPIS measures will allow the information systems of the organisation to perform (to a certain degree) even in complex situations. Moreover, many respondents think that CPIS measures in their organisations are kept current. This is indicated by the high mean response of 3.43. Despite these findings, many respondents still believe that the responsibility for the CPIS in their organisations lies with the IT or the IS department.

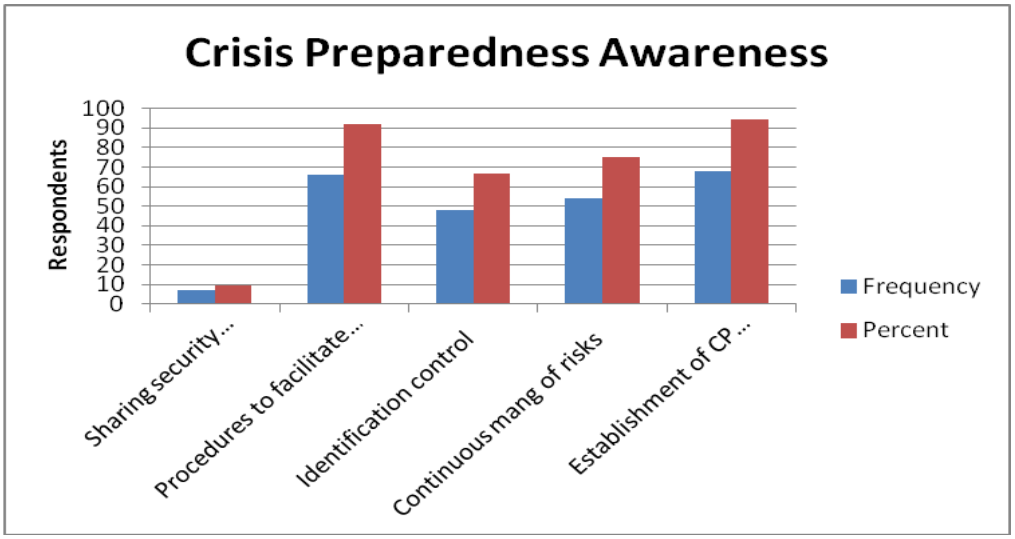

Figure 2.16: Crisis Preparedness Awareness - Statistics

The data on Figure 2.16 indicate that above 60% of the respondents are aware of and understand different processes and procedures related to the preparedness of the information systems within their organisation. These include (1) procedures that facilitate the restoration of the information systems after a crisis event, (2) identification, control and mitigation of IS risks and threats, (3) continuous management of risks and (4) establishment of crisis preparedness plans.

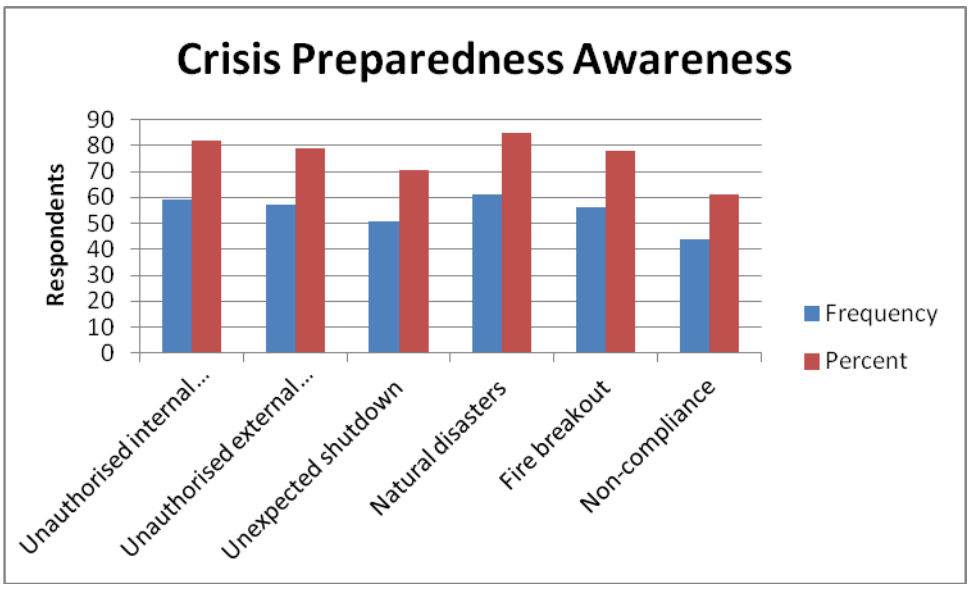

Figure 2.17: Crisis Preparedness Awareness - Statistics

Figure 2.17 shows that above 60% of the respondents are aware of the common adverse events that may lead to negative consequences to the information systems of the organisation. These include unauthorised internal access, unauthorised external access, unexpected system shutdown, and non compliance, among others.

4.8 Pearson's Correlation Coefficients of the Variables

In order to understand the association between sets of variables, Pearson's Correlation Coefficient analysis was adopted. Resulting from this analysis were the Pearson's Coefficient of Correlation (r) and the values of significance (*p*).

The analyses of the association between sets of variables including the research hypotheses that generated them follow next.

End-users' intention to comply with the measures for CPIS within the organisation is likely to be positively influenced by their attitude of crisis preparedness of the information systems.

From this hypothesis, a set of five variables was generated. These included ATTC1, ATTC2, ATTC3, ATTC4 and ATTC5.

Table 4.14: Correlations - Attitude Towards CPIS

		ATTC1	ATTC2	ATTC3	ATTC4	ATTC5
ATTC1	R	1				
	Sig. (2-tailed)					
	N	70				
ATTC2	R	**.279***	1			
	Sig. (2-tailed)	.022				
	N	67	67			
ATTC3	R	-.077	**-.504****	1		
	Sig. (2-tailed)	.535	.000			
	N	67	67	67		
ATTC4	R	**.407****	**.289***	-.153	1	
	Sig. (2-tailed)	.001	.024	.239		
	N	61	61	61	61	
ATTC5	R	**-.518****	-.222	.183	**-.338****	1
	Sig. (2-tailed)	.000	.071	.139	.008	
	N	70	67	67	61	70
***. Correlation is significant at the 0.05 level (2-tailed).**						
****. Correlation is significant at the 0.01 level (2-tailed).**						

Table 4.14 shows four correlations with attitude towards CPIS with different significant levels. First, the variable ATTC2, "incorporation of crisis preparedness activities into day to day activities" correlates weakly ($r = .279$, $p < .05$) with the variable ATTC1, "CPIS is a responsibility for all employees". This means that CPIS is likely to be effective if its responsibility is assumed by all employees and it is integrated into day to day activities. On the other hand, the variable ATTC5, "CPIS is the responsibility of a selected group of people" correlates moderately ($r = -.518$, $p < .01$) with the variable ATTC1, "CPIS is the responsibility all employees". This means that if a selected group of people is replaced by end-users then end-users are likely to comply with CPIS measures. This is because CPIS now becomes part and parcel of their daily duties.

Moreover, ATTC3 correlates modestly with ATTC2 ($r = -.504$, $p < .01$), ATTC4 correlates moderately with ATTC1 ($r = .407$, $p < .01$) and ATTC4 correlates weakly with ATTC2 ($r = .289$, $p < .05$).

Normative expectations about the crisis preparedness of the information systems are likely to affect end-users' intentions to comply with the measures for CPIS within the organisation.

From this hypothesis a set of four variables was generated. These included NE1, NE2, NE3 and NE4.

Table 4.15: Correlations - Normative Expectations

		NE1	NE2	NE3	NE4
NE1	R	1			
	Sig. (2-tailed)				
	N	61			
NE2	R	-.209	1		
	Sig. (2-tailed)	.105			
	N	61	61		
NE3	R	.011	-.046	1	
	Sig. (2-tailed)	.939	.745		
	N	53	53	53	
NE4	R	-.033	-.145	**.760****	1
	Sig. (2-tailed)	.813	.301	.000	
	N	53	53	53	53

****. Correlation is significant at the 0.01 level (2-tailed).**

Test results reported in Table 4.15 exhibit one significant correlation with normative expectations. The variable NE4, "CP training and communication allow working together" correlates strongly ($r = .760, p<.01$) with the variable NE3, "training provide the know how in crisis events". This means that crisis preparedness training and communication are likely to facilitate combined efforts from end-users to adhere to established measures for the CPIS.

End-users' intentions to comply with CPIS measures are likely to have a significant impact on actual compliance with CPIS measures.

From this hypothesis a set of five variables was generated. These included ITC1, ITC2, ITC3, ITC4 and ITC5.

Table 4.16: Correlations - Intention to Comply

		ITC1	ITC2	ITC3	ITC4	ITC5
ITC1	R	1				
	Sig. (2-tailed)					
	N	62				
ITC2	R	.151	1			
	Sig. (2-tailed)	.254				
	N	59	59			
ITC3	R	.139	**.489****	1		
	Sig. (2-tailed)	.295	.000			
	N	59	59	59		
ITC4	R	-.071	.240	**.319***	1	
	Sig. (2-tailed)	.591	.067	.014		
	N	59	59	59	59	
ITC5	R	-.112	.236	**.360****	.116	1
	Sig. (2-tailed)	.399	.073	.005	.382	
	N	59	59	59	59	59
****. Correlation is significant at the 0.01 level (2-tailed).**						
***. Correlation is significant at the 0.05 level (2-tailed).**						

Table 4.16 shows three significant correlations with intention to comply. The first indicate the likelihood of end-user compliance by keeping strong passwords (ITC3) and changing them on a regular basis (ITC2) to prevent unauthorised access to secure systems. The variables ITC3 and ITC2 correlate moderately with a Pearson's coefficient of .489 ($p<.01$). Second, the variable ITC4, "strict information access" correlates weakly ($r = .319, p<.05$) with the variable ITC3, "ensuring strong passwords". This means that end-users are likely to adhere to strict information access controls if they apply strong secure passwords. Thirdly, the variable ITC5, "regular back up of data" correlates modestly ($r = .360, p<.01$) with the variable ITC3, "ensuring strong passwords". This means that data recovery after a crisis event is likely to be effective if end-users kept backed up data under secure passwords. In other words the data won't be compromised during and after a crisis event.

Threat appraisal affects end-users' intention to comply with the established measures for CPIS within the organisation.

From this hypothesis a set of four variables was generated. These included TA1, TA2, TA3 and TA4.

Table 4.17: Correlations - Threat Appraisal

		TA1	TA2	TA3	TA4
TA1	Pearson Correlation	1		.	
	Sig. (2-tailed)				
	N	62			
TA2	Pearson Correlation	-.124	1		
	Sig. (2-tailed)	.348			
	N	59	59		
TA3	Pearson Correlation	.213	**.350****	1	
	Sig. (2-tailed)	.106	.007		
	N	59	59	59	
TA4	Pearson Correlation	-.095	.035	.011	1
	Sig. (2-tailed)	.472	.792	.934	
	N	59	59	59	59

****. Correlation is significant at the 0.01 level (2-tailed).**

Table 4.17 exhibits one significant correlation with threat appraisal. The variable TA3, "Non compliance is a serious issue" correlates weakly ($r = .350, p<.01$) with the variable TA2, "lack of adherence will lead to negative consequences".

Response efficacy affects end-users' intentions to comply with the established measures for the CPIS within the organisation.

From this hypothesis a set of seven variables was generated. These included RE1, RE2, RE3, RE4, RE5, RE6 and RE7.

Table 4.18: Correlations - Response Efficacy

		RE1	RE2	RE3	RE4	RE5	RE6	RE7
RE1	r	1						
	Sig. (2-tailed)							
	N	44						
RE2	r	**.635****	1					
	Sig. (2-tailed)	.000						
	N	44	61					
RE3	r	**.536****	**.535****	1				
	Sig. (2-tailed)	.000	.000					
	N	44	61	61				
RE4	r	-.214	-.096	-.131	1			
	Sig. (2-tailed)	.163	.465	.318				
	N	44	60	60	60			
RE5	r	**-.375***	**-.367****	**-.256***	.229	1		
	Sig. (2-tailed)	.012	.004	.049	.078			
	N	44	60	60	60	60		
RE6	r	**.382***	.151	.244	-.144	**-.324***	1	
	Sig. (2-tailed)	.016	.281	.078	.303	.018		
	N	39	53	53	53	53	53	
RE7	r	**.454****	.204	.188	-.221	**-.376****	**.603****	1
	Sig. (2-tailed)	.004	.144	.178	.112	.006	.000	
	N	39	53	53	53	53	53	53
****. Correlation is significant at the 0.01 level (2-tailed).**								
***. Correlation is significant at the 0.05 level (2-tailed).**								

Table 4.18 exhibits several significant correlations with response efficacy. The level of CPIS in the organisation (RE2) correlates moderately ($r = .635$, $p<.01$) with the CPIS improvements that have been made after the last known event (RE1). On the other hand, the variable RE7, "CP training introduced end-users to available resources and tools" correlates moderately ($r = .603$, $p<.01$) with the variable RE6, "CP training involves simulation of potential adverse events". This may imply that end-users' response efficacy is likely to enhance the identification of IS risks and threats and mitigate them effectively before they develop into negative consequences to the information systems.

Self-efficacy affects end-users' intentions to comply with established measures for CPIS within the organisation.

A set of seven variables was generated from this hypothesis. They included SE1, SE2, SE3, SE4, SE5, SE6 and SE7.

Table 4.19: Correlations - Self Efficacy

		SE1	SE2	SE3	SE4	SE5	SE6	SE7
SE1	R	1						
	Sig. (2-tailed)							
	N	62						
SE2	R	**.444****	1					
	Sig. (2-tailed)	.000						
	N	61	61					
SE3	R	.196	**.455****	1				
	Sig. (2-tailed)	.134	.000					
	N	60	60	60				
SE4	R	-.242	**-.334****	**-.544****	1			
	Sig. (2-tailed)	.062	.009	.000				
	N	60	60	60	60			
SE5	R	**-.256***	-.247	**-.377****	**.596****	1		
	Sig. (2-tailed)	.048	.057	.003	.000			
	N	60	60	60	60	60		
SE6	R	.206	**.388****	.178	-.120	-.166	1	
	Sig. (2-tailed)	.115	.002	.174	.362	.205		
	N	60	60	60	60	60	60	
SE7	R	**.344***	.259	.162	-.263	**-.442****	**.363****	1
	Sig. (2-tailed)	.012	.061	.247	.057	.001	.008	
	N	53	53	53	53	53	53	53
****. Correlation is significant at the 0.01 level (2-tailed).**								
***. Correlation is significant at the 0.05 level (2-tailed).**								

Table 4.19 exhibits a number of significant correlations with self efficacy. The variable SE5, "fixed training schedules" correlates moderately ($r = .596$, $p<.01$) with the variable SE4, "CP measures are reviewed after certain intervals". This means that organisations which have fixed training schedules with regard to CPIS are likely to review their CPIS measures at established intervals. In addition, the variable SE4, "CPIS measures are reviewed at certain intervals" correlates moderately ($r = -.544$, $p<.01$) with the variable SE3, "CPIS measures are operational". This means that organisations which have integrated CPIS measures into their daily operations are unlikely to review CPIS measures by following fixed schedules. In

other words, they are likely to review their CPIS measures more often because it is integrated into their daily operations.

Crisis preparedness awareness positively influences end-users' intentions to comply with established measures for CPIS within the organisations.

A set of eight variables was generated from this hypothesis. However, the following variables: CPA1, CPA2, CPA4, and CPA5 seemed to produce constant values in the calculation for the Pearson's Coefficient Correlation. Hence, they were not included in this computation. The correlation analysis for this hypothesis only included the following variables: CPA3, CPA6, CPA7 and CPA8.

Table 4.20: Correlations - Crisis Preparedness Awareness

		CPA3	CPA6	CPA7	CPA8
CPA3	R	1			
	Sig. (2-tailed)				
	N	70			
CPA6	R	-.155	1		
	Sig. (2-tailed)	.228			
	N	62	62		
CPA7	R	.116	.086	1	
	Sig. (2-tailed)	.378	.514		
	N	60	60	60	
CPA8	R	.156	-.125	**.301***	1
	Sig. (2-tailed)	.235	.340	.020	
	N	60	60	60	60

***. Correlation is significant at the 0.05 level (2-tailed).**

Table 4.20 exhibits one significant correlation with crisis preparedness awareness. The variable CPA8, "CP measures are kept current" correlates weakly ($r = .301$, $p<.05$) with the variable CPA7, "CP measures allow performance even in uncertainty". This may imply that if organisations keep their CPIS measures current then these measures are likely to facilitate the information systems platforms ability to function (at least to some degree) in crisis situations. In other words, end-users' understanding and awareness of the CPIS strategies within their organisations are likely to influence their actual compliance (actions) with these measures even in times of uncertainty.

4.9 Chapter Summary

This chapter presented the data analysis and described the research findings. Information about the survey respondents and the process that was used to acquire them was provided. This included the information about the organisations that were approached and different communication methods that were used to request their participation in the study. The process of preparing the data, the response rate and the demographics were described in details.

The demographics section was followed by the reliability tests, the descriptive statistics analyses and the correlation analyses. The correlation analyses presented the Pearson's Coefficient of Correlations for different sets of variables, including their values of significance.

Chapter 5: Discussion and Conclusion

5.1 Introduction

This chapter sums up key points and statements from the four chapters of this thesis. The path undertaken by the researcher from the identification of the research gap to the main findings of the study is presented. This chapter also includes the implications of the study and the main contributions of the research from both academic and practitioner perspectives. This is followed by the limitations of the study in relation to the research design, the research instrument and the data collection process. Finally, opportunities for future research are suggested.

5.2 Overview of the Research

5.2.1 Research Gap

Despite the existence of different measures to counteract crisis events in organisations, the frequency and magnitude of these events remain high in the recent past (Hu et al., 2006; Jain & Singh, 2012). This was particularly of interest given the low figures of crisis preparedness on a global scale reported in diverse studies such as Susanto (2003) and Ernst and Young (2003). Some identified challenges with crisis-preparedness were linked to lack of understanding or awareness of fundamental components of crisis-preparedness of the information systems particularly from the end-user's perspective (Siponen, 2000; Susanto, 2003). Added to the list were the human behaviours such as attitudes and perceptions (Garrett, 2004; Rhee & Kim, 2005) in relation to different measures established by organisations toward crisis preparedness endeavours.

For these reasons, two research questions were identified in an attempt to fill the research gap. They included:

1) ***What is the extent of end-user awareness of crisis preparedness of the information systems within the organisation?***

2) ***What is the extent of end-user adherence to crisis preparedness of the information systems in the organisation?***

5.2.2 Research Objectives and Hypotheses

Research objectives are fundamental to ensuring that the underlying research question(s) are appropriately addressed. The review of relevant publications from IS and other reference disciplines suggested that the low level of crisis preparedness of the information systems in organisations may have a direct link to lack of end-user understanding, and a lack of both end-user awareness of and adherence to CPIS measures. In line with this argument and the identified research questions, the research objectives for this study were to:

- determine the key elements of the CPIS;
- determine the extent of end-user awareness of the CPIS measures in their organisations;
- determine the extent of end-user adherence to CPIS measures established within the organisation; and
- apply two existing theories to analyse the collected data on end-user awareness of and adherence to CPIS measures in New Zealand organisations.

However, to answer the research questions fully it was necessary to generate and test research hypotheses. The research hypotheses were generated on the basis of two theoretical frameworks: the Theory of Reasoned Action (TRA) and the Protection Motivation Theory (PMT). The choice of these two theoretical frameworks was driven by the appropriateness of their key assumptions to this study. For instance, the assumption that behaviour is best predicted by intention was relevant when examining the degree to which end-users were prepared to apply or not to apply established measures for CPIS in their organisations. On the other hand, the PMT framework was a relevant choice for this study due to its applicability in situations that involve threats and for which there is an expectation from peers or managers that end-users should act in a certain way. In other words, the PMT allowed the researcher to examine the belief that motivation toward protection is inherent in perceived IS threats and risks and the need to avoid the potential negative outcomes (*please refer to chapter 4 for detailed analysis*).

From the TRA and the PMT theoretical frameworks, six variables out of seven were chosen for this study: attitude towards CPIS, normative expectations, intention to comply, threat appraisal, response efficacy, and self efficacy. The seventh variable: crisis preparedness awareness was devised as a new scale variable for this study.

From these variables seven research hypotheses were generated in an attempt to answer the research questions identified at the start of this study. The research hypotheses were as follows:

- *End-users' intention to comply with the measures for CPIS within the organisation is likely to be positively influenced by their attitude of crisis preparedness of the information systems.*

- *Normative expectations about the crisis preparedness of the information systems are likely to affect end-users' intentions to comply with measures for CPIS within the organisation.*

- *End-users' intentions to comply with CPIS measures are likely to have a significant impact on actual compliance with CPIS measures.*

- *Threat appraisal affects end-users' intention to comply with established measures for CPIS within the organisation.*

- *Response efficacy affects end-users' intentions to comply with established measures for CPIS within the organisation.*

- *Self-efficacy affects end-users' intentions to comply with established measures for CPIS within the organisation.*

- *Crisis preparedness awareness positively influences end-users' intentions to comply with established measures for CPIS within the organisations.*

5.2.3 Research Design

In order to accomplish the research objectives and to answer the research questions, a quantitative positivist research method was adopted for this study. This approach was appropriate to generate facts about the crisis preparedness of information systems in New Zealand organisations without requiring subjective interpretation.

Even though the three respondent organisations were tied up with busy roadmaps of compliance projects, still they found it beneficial to permit their employees to participate in the study. Nevertheless, this was a disappointment that only three organisations agreed to participate in the study. It could have been a greater success if more organisations had agreed to the study request.

In consultation with a representative from each respondent organisation, it was agreed that potential participants should be identified from all departments across the organisation. Hence, study participants were identified from a cross section of employees that used information systems applications over their desktop computers or from their mobile devices. These are the people that used these kinds of systems to perform their daily duties. However, the researcher had no control over the participants selection process; hence it is possible that the sample was purposively identified (i.e. a judgemental sample). This is because the sample was selected based on certain criteria or some characteristics known only to the organisations themselves.

From the three participating organisations a total number of 297 email invitations were sent out. The email invitation (see *Appendix C.2*) was followed by a second email message (see *Appendix C.3*) which contained instructions about the survey to the respondents. This email message also contained a web-link that gave access to an anonymous web-based survey. Three weeks into the study, a reminder email message (see *Appendix C.4*) was sent out to all invitees. This was necessary to encourage those who were interested to take part in the study to do so and those who had not completed their responses to do so before the study came to a close. Given the low response rate, it was necessary to send out a second reminder six weeks into the study. The two reminder emails gave a small boost to the response rate.

The collected data was analysed from three different approaches. Data analyses using descriptive statistics and percentage responses were necessary to ascertain facts about crisis preparedness of the information systems in New Zealand organisations. Correlation analyses were performed on the collected data in order to understand the relationships between different sets of variables.

5.3 Study Implications

The most important implication for both academia and practice is the understanding that greater emphasis should be given to the processes that bring about the CPIS strategies across varying organisation structures.

Attitude towards CPIS, referring to the degree to which end-users perceive the importance of their contribution to the effectiveness of the CPIS measures, will be manifested in their intention to comply with the measures for CPIS. This finding suggests the importance of establishing processes that will see the responsibility for the CPIS being distributed across the entire community of the organisation. This is because many of the respondents were of the opinion that responsibilities for the crisis preparedness of their systems belong only to the Information Technology or the Information Systems departments. This was unexpected, especially from end-users that have gone through deliberate training associated with CPIS measures. The findings also suggest that IS practitioners should emphasise to their colleagues that many of the crisis incidents originate from within. Hence, it is the task of every employee to be vigilant on likely IS threats and risks so as to achieve effective crisis preparedness of the information systems.

Study results show that normative expectations have a significant effect on end-users' intentions to comply with the measures for CPIS within the organisation. This finding stresses the significance of providing knowledge to all employees about countermeasures to crisis events. If employees have not been exposed to the facts and skills for handling crisis events, they will find it difficult to know what is expected of them. One respondent notes that, "we have recently (since the Christchurch earthquake) established a framework to assist users to determine their … requirements." This observation suggests that if end-users are brought to the same level of understanding, it would be easier for them to comply with the measures for CPIS because that is what her/his peers, colleagues and managers expect of them.

Intentions to comply, signifying end-users' willingness to attempt to perform a given behaviour, will lead them to actual compliance with CPIS measures. This finding suggests that organisations should provide informative sessions to end-users about different CPIS strategies in their organisations. This will enlighten the end-users on why they should adhere to CPIS measures. While educating all employees within the organisation may seem expensive, the study results indicate that end-users will comply with CPIS measures if they perceive the importance of those measures to the IS platforms.

Study findings indicate that threat appraisal has a significant impact on end-users' intention to comply with established measures for CPIS within the organisation. In other words, perceived vulnerability and perceived severity about non compliance with CPIS will be manifested in end-users' intentions to adhere to established measures for CPIS. From the IS practitioners view, a few points are worth mentioning here. First, all employees should be made aware of IS threats and risks that can potentially affect the IS platforms of the organisation. As the results indicate, many respondents were unaware of this critical information. More precisely, it has not been communicated to them. Second, all employees should be made to understand that IS threats and risks are real. This is because study results show that many respondents didn't accept the idea that their organisations can encounter some of the IS risks and threats common to IS. Third, awareness programmes should be conducted for the purposes of educating end-users about the severity and seriousness posed by crisis events to the organisation's wellbeing. Employees need to know that the financial implications and the lost integrity of the organisation's systems resulting from adverse events are enormous while the threat to information systems is relentlessly rising.

Response-efficacy, signifying end-users' beliefs in the perceived benefits of the coping action will improve their intentions to comply with CPIS measures within their organisations. This finding underlines the perceived relevance of the CPIS strategies. If end-users don't perceive CPIS measures as important and adequate enough to offset impending threats, they will not adhere to those measures. This finding suggests to the IS practitioners that it is essential to enlighten end-users through awareness programmes such as workshops and event simulations about the capabilities and the functionalities of the crisis event countermeasures. Several respondents' also note the importance of conducting sessions like: mock system restores, backup retrieval, and testing CPIS procedures. In doing so, end-users will be aware of different resources and tools to use given the crisis event.

Research results show that end-users' self efficacy has a significant impact on their intentions to comply with established measures for CPIS within the organisation. The findings from this study indicate that IS practitioners should ensure that end-users are given the assurance that they are capable of carrying out CPIS measures. This can be done by providing information on any reviewed CPIS strategies such as what has been changed and how the end-user fits into the new way of doing things. In this way the spur and the confidence of end-users to apply CPIS measures in their daily duties will be uplifted. In other words, the review of CPIS measures should go hand in hand with training and awareness programmes for the end-users.

Crisis preparedness awareness refers to the degree to which end-users' knowledge and understanding of different aspects of CPIS in their organisation will lead to end-users' intentions to comply with established measures for CPIS within their organisation. To the IS practitioners this implies that end-users should be to the fore with regard to CPIS measures. Key areas that IS practitioners should consider in order to ensure that end-users are at the centre of organisational efforts as far as CPIS measures are concerned include (1) forging relationships between stakeholders, (2) sharing information about risks and threats they come across on a daily basis, (3) being severe on unsafe activities or practices, (4) being aware of the processes and procedures to follow in the event of a crisis.

The general study implications as outlined in this section are further complemented by research contributions for both academics and practitioners. These contributions are presented next.

5.4 Contributions of this Research

The contributions made by this research to the existing body of knowledge can be viewed from two perspectives. First are the contributions that in this text are referred to as "academic contributions" and the other contributions are those which are termed as "practitioner contributions". Selected examples about these two types of contributions are elaborated in more detail in the next two sections.

5.4.1 Academic Value of the Research

The primary value of this research to academia is the expansion of the existing discourse on crisis-preparedness. This was accomplished by the application of existing theories (i.e. TRA

and PMT) to analyse the collected data. The consolidation of these theoretical frameworks and their application to analyse the quantitative data added knowledge to the field of crisis-preparedness in IS.

Secondly, this is the first study in New Zealand that has empirically examined the crisis preparedness of information systems in organisational settings. This was accomplished by capturing end-user perceptions on forty one (41) items which were later used to test the research hypotheses.

A third contribution of this study is the development of a questionnaire tool which integrates a cluster of statements describing facets of seven different dimensions of CPIS. At the analysis stage each dimension became one of the seven variables: *attitude towards CPIS, normative expectations, intention to comply, threat appraisal, response efficacy, self efficacy* and *crisis preparedness awareness*. Six of these variables have been used in combination with other variables in existing measures or instruments. However, the *crisis preparedness awareness* dimension and hence the variables were newly created, including the amalgamation of the seven variables to create measures for CPIS.

A fourth contribution is the testing of the seven variables in the context of the crisis preparedness of the information systems. This is because none of these variables had previously been tested in this context.

A fifth contribution is that this study used participants from the actual working environment as opposed to other studies that use students as participants (Sivo et al., 2006). This is because some studies use student participants in order to increase the external validity of their instruments. Sivo et al., argue that the representativeness of the sample is pertinent to ensure for external validity in a given study. In other words, study findings based on a sample drawn from the actual population are more applicable in IS research regardless of a smaller sample size. Therefore, the findings from this study can be generalised to a wider population because the respondents gave their opinions based on the actual systems, actual structures and actual organisational processes and procedures with regards to CPIS.

5.4.2 Practitioner Value of the Research

This study also offers value to the practitioner community. The significance of the results from this study allow the practitioner community to gain a better understanding of the level of end-user awareness of and adherence to crisis preparedness of the information systems in their organisations. From this understanding, organisations are able to improve or enhance user participation in crisis preparedness of the information systems at all levels.

A second contribution to IS practitioners is the availability of a valid and reliable tool with which organisations can assess the crisis preparedness of their information systems against a wide range of IS threats and risks. Previously, organisations could assess their vulnerability to potential IS threats and risks by applying up to four different strategies. These include business continuity plans, disaster recovery plans, information systems security and information systems risk management. However, the tool created for this project is very important to organisations because now they can assess the status or progress of their crisis preparedness initiatives in just one step.

The third contribution is that the findings from this study can act as a catalyst to implement enhanced CPIS measures for organisations that have not implemented such measures yet.

5.5 Limitations of the Study

Despite the benefits drawn from the research findings, the researcher would like to acknowledge some limitations associated with this study. Study limitations are grouped in three different categories: the research design, the research instrument and the data collection process. The next three sections discuss each limitation category in more detail.

5.5.1 Limitations of the Research Design

Despite the number of benefits offered by a web-based survey such as cost reduction and processing time, the downside is that a web-based survey may suffer coverage limitations (Sivo et al., 2006). This is because the survey web-link was meant to be completed by participants with access to the Internet on their workstation computers or mobile devices. However, potential participants might have been left out because they had restricted access to Internet on their workstation computers. This is because in some organisations employees are

only allowed to access the Internet during the lunch break. It is likely that in that half hour lunch break the survey had to compete for attention with other favourite sites like Facebook and Twitter.

Again, this study took place at a time when the negative consequences from some major crisis events in New Zealand such as Pike River Mine and Christchurch earthquake were still fresh in the minds of managers and executives. The timing of the study perhaps was not right as managers in some organisations might have had a feeling that their unpreparedness would be exposed.

The data was predominantly collected from the two large New Zealand cities: Wellington and Auckland. An interesting follow-up study would be to collect data from a random sample of organisations from different cities across New Zealand.

5.5.2 Limitations of the Research Instrument

The positivist research paradigm adopted for this study is known to pose some limitations (Lincoln & Guba, 1985) in presenting a complete picture of information systems phenomena (Orlikowski & Baroudi, 1991). This is because the positivist research approach has a tendency to discount the historical context of phenomena on human actions. While the survey instrument used for this study attempted to capture both end-user awareness of and adherence to CPIS, but did not explore how social contexts, marked by time, locale, organisation politics, and organisation culture may have influenced end-users responses (Orlikowski & Baroudi, 1991). The social contexts were not considered in the data capturing process as they were outside the scope of this study.

Both internal and external validity of the research instrument cannot be claimed as this study is descriptive. The two major concerns were only to ensure quality and credibility of the study and that the study findings can be generalised to a wider population.

The reliability coefficients scales for the five variables: attitude towards CPIS, intention to comply, threat appraisal, self efficacy and crisis preparedness awareness were below the normal standard alpha of 0.7. Further refinement of these scales can be of benefit for future studies.

5.5.3 Limitation of the Data Collection Process

The numbers of employees allowed to participate into the study were restricted by the respondent organisations.

Since the respondent organisations had a control on who could participate into the study, it is likely the sample is not random. This may limit the generalisability of the findings. In addition, the sample size remains relatively low. A larger sample size could have provided more accurate statistical evidence.

Prior research studies on user awareness and adherence had investigated business continuity, disaster recovery, systems risk management, and information security as separate domains. However, this study examined these domains as a single entity of crisis preparedness of the information systems (CPIS). Moreover, the researcher also assumed the same combination of these domains (i.e. BCP, DRP, ISS and ISRM) to exist across all respondent organisations.

5.6 Future Research

This study presents other opportunities for further research. Although the variables utilized in this study were drawn from TRA and PMT, the analysis does not attempt to change the current configuration of each of these theoretical frameworks. This study only tested the association among the variables through the use of the Pearson's Correlation Coefficients. Future studies can be designed around producing a model and test for causality among the variables.

Again, further quantitative research, using a somewhat similar survey instrument, could be carried out to validate and confirm the results acquired in this study. That can be done after incorporating some of the recommendations/suggestions provided by respondents in this current study. Another alternative is to broaden the scope of the study by including more countries, organisation cultures, and the institutionalisation of CPIS strategies to validate and extend the findings of the present study.

This study integrates different aspects of the TRA with PMT to generate seven research hypotheses for the study. Future studies may substitute the TRA with the Theory of Planned Behaviour (Ajzen, 1991), which extends TRA. The Theory of Planned Behaviour brings in a perceived behavioural control component to TRA. This component is in-line with the concept that "successful performance of the intended behaviour is contingent on the person's control over the many factors that may prevent it"(Ajzen, 2005, p. 110), and it thus embraces practical constraints that may be present.

5.7 Chapter Summary

This is the chapter that brings us to a close of the thesis. A concise summary of the research process was first provided. This summarised the important aspects leading up to the core findings of the study. The research gap, the research objectives and hypotheses and the research design were all outlined. This was followed by a discussion on the study implications and the research contributions from both academia and practice perspectives.

The limitations of the study were then discussed. These were categorised into three groups: limitations pertaining to the study design, limitations pertaining to the research instrument and the data collection process. Finally, opportunities for future research were suggested.

References

Ajzen, I, & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour*. Englewood Cliffs:Prentice-Hall.

Ajzen, Icek. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Ajzen, Icek. (2005). *Attitudes, Personality and Behavior 2e*. McGraw-Hill International.

Alam, I. (2005). Fieldwork and data collection in qualitative marketing research. *Qualitative Market Research: An International Journal*, *8*, 97–112. doi:10.1108/13522750510575462

Albani, J. (2011). Information Security Guideline - NSW Government DFS. Retrieved December 29, 2011, from http://services.nsw.gov.au/inside-dfs/information-communications-technology/publications/information-security-guideline

Alexander, D. (2005). Towards the development of a standard in emergency planning. *Journal of Contingencies & Crisis Management*, *14*, 158–175. doi:doi:10.1108/09653560510595164

Allen, J. (2005). Governing for Enterprise Security. Retrieved December 1, 2011, from http://www.sei.cmu.edu/library/abstracts/reports/05tn023.cfm

Al-Zarouni, M. (2006). The Reality of Risks from Consented use of USB Devices. *Australian Information Security Management Conference*. Retrieved from http://ro.ecu.edu.au/ism/70

Applegate, L. M. (1999). *Corporate Information Systems Management: Text and Cases* (5th ed.). Boston: Irwin/McGraw-Hill.

Armstrong, C. P., & Sambamurthy, V. (1999). Information Technology Assimilation in Firms: The Influence of Senior Leadership and it Infrastructures. *Information Systems Research*, *10*, 304–327. doi:http://dx.doi.org/10.1287/isre.10.4.304

Australian Communications & Media Authority. (2008). Developments in internet filtering technologies and other measures for promoting online safety. Report. Retrieved August 1, 2012, from http://www.egov.vic.gov.au/focus-on-countries/australia/trends-and-issues-australia/telecommunications-australia/developments-in-internet-filtering-technologies-and-other-measures-for-promoting-online-safety-2nd-report-in-pdf-format-3176kb-.html

Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions. Dependable and Secure Computing*, *1*(1), 11–33. doi:10.1109/TDSC.2004.2

Aydin, C. E., & Rice, R. E. (1991). Social worlds, individual differences, and implementation: Predicting attitudes toward a medical information system. *Information and Management*, *20*(2), 119–136. doi:10.1016/0378-7206(91)90049-8

Aytes, K., & Conolly, T. (2003). A Research Model for Investigating Human Behavior Related to Computer Security. *AMCIS 2003 Proceedings*. Retrieved from http://aisel.aisnet.org/amcis2003/260

Bagozzi, R. (1980). Causal Models in Marketing. *The Journal of Marketing*, *44*(4), 126–128. doi:10.2307/1251239

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215.

Banerjee, M. M., & Gillespie, D. F. (1994). Linking Disaster Preparedness and Organizational Response Effectiveness. *Journal of Community Practice*, *1*(3), 129. doi:10.1300/J125v01n03_09

Baroudi, J. J., & Orlikowski, W. J. (1988). A Short Form Measure of User Information Satisfaction: A Psychometric Evaluation and Notes on Use. *SSRN eLibrary*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1289738

Bharadwaj, A. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly*, *24*(1), 169. doi:10.2307/3250983

Boin, A., & Lagadec, P. (2000). Preparing for the Future: Critical Challenges in Crisis Management. *Journal of Contingencies and Crisis Management*, *8*(4), 185–191. doi:10.1111/1468-5973.00138

Botha, J., & Solms, R. V. (2004). A cyclic approach to business continuity planning. *Information Management & Computer Security*, *12*(4), 328–337. doi:10.1108/09685220410553541

Boudreau, M.-C., Gefen, D., & Straub, D. (2004). Validation Guidelines for IS Positivist Research. *Communications of the Association for Information Systems*, *13*(1). Retrieved from http://aisel.aisnet.org/cais/vol13/iss1/24

Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in Information Systems Research: A State-of-the-Art Assessment. *MIS Quarterly*, *25*(1), 1–16. doi:10.2307/3250956

Boyer, K. K., Olson, J. R., Calantone, R. J., & Jackson, E. C. (2002). Print versus electronic surveys: A comparison of two data collection methodologies. *Journal of Operations Management*, *20*(4), 357–373. doi:16/S0272-6963(02)00004-9

Broadbent, M., & Weill, P. (1997). Management by Maxim: How Business and IT Managers Can Create IT Infrastructures. http://purl.org/dc/dcmitype/Text. Retrieved May 15, 2011, from http://dialnet.unirioja.es/servlet/articulo?codigo=2509669

Brown, L. M., Hickling, E. J., & Frahm, K. (2010). Emergencies, Disasters, and Catastrophic Events: The Role of Rehabilitation Nurses in Preparedness, Response, and Recovery. *Rehabilitation Nursing*, *35*(6), 236.

Bryman, A. (2008). *Social Research Methods* (3rd ed.). OUP Oxford.

Caponigro, J. R. (2000). *The Crisis Counselor: A Step-By-Step Guide to Managing a Business Crisis* (First Edition.). McGraw-Hill Companies.

Cerullo, V., & Cerullo, M. J. (2004). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management*, *21*(3), 70.

Chang, J. C.-J., & King, W. R. (2005). Measuring the Performance of Information Systems: A Functional Scorecard. *Journal of Management Information Systems*, *22*(1), 85–115.

Chow, W. S., & Ha, W. O. (2009). Determinants of the Critical Success Factor of Disaster Recovery Planning for Information Systems. *Information Management & Computer Security*, *17*(3), 248–275. doi:10.1108/09685220910978103

Coleman, L. (2006). Frequency of Man-Made Disasters in the 20th Century. *Journal of Contingencies and Crisis Management*, *14*(1), 3–11. doi:10.1111/j.1468-5973.2006.00476.x

Computer Emergency Response Team. (2001). Denial of Service. Retrieved August 4, 2012, from http://www.cert.org/tech_tips/denial_of_service.html#1

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ED.). Sage Publications.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, *20*(1), 79–98,155,157.

Denis, H. (1995). Scientists and disaster management. *Disaster Prevention and Management*, *4*(2), 14–19. doi:10.1108/09653569510082650

Denzin, N. K., & Lincoln, Y. S. (2005). Introduction: The Discipline and Practice of Qualitative Research. In *The SAGE Handbook of Qualitative Research* (3rd ed.). Thousand Oaks Calif.: SAGE.

Eaglestone, B., Lin, A., Nunes, M. B., & Annansingh, F. (2003). Intention and Effect of IS Solutions: Does Risk Management Stifle Creativity? *Journal of Information Science, 29*(4), 269–278. doi:10.1177/01655515030294004

Elky, S. (2006). An introduction to Information System Risk Management. Retrieved December 1, 2011, from http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204

Elliott, D., & Smith, D. (2006). Cultural Readjustment After Crisis: Regulation and Learning from Crisis Within the UK Soccer Industry. *Journal of Management Studies, 43*(2), 289–317. doi:10.1111/j.1467-6486.2006.00591.x

Elsubbaugh, S., Fildes, R., & Rose, M. B. (2004). Preparation for Crisis Management: A Proposed Model and Empirical Evidence. *Journal of Contingencies and Crisis Management, 12*(3), 112–127. doi:10.1111/j.0966-0879.2004.00441.x

Ernst & Young. (2002). Global Information Security Survey 2002. Retrieved November 30, 2011, from http://www.passwordresearch.com/stats/study18.html

Ernst & Young. (2003). Global Information Security Survey 2003. Retrieved July 21, 2012, from http://www.itsmportal.com/news/global-information-security-survey-2003

Evans, N. (2003). Information Security Guideline for NSW Government Agencies. Retrieved December 29, 2011, from www.albany.edu/acc/courses/ia/inf766/nswinfosecriskmanagementpt11997.pdf

Faulkner, B. (2001). Towards a framework for tourism disaster management. *Tourism Management, 22*(2), 135–147. doi:10.1016/S0261-5177(00)00048-0

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Addison-Wesley Pub. Co.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology, 30*(2), 407–429. doi:10.1111/j.1559-1816.2000.tb02323.x

FTC. (2006). Choicepoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress. Retrieved November 27, 2011, from http://164.62.13.221/opa/2006/01/choicepoint.shtm

Furnell, S., & Phyo, A. H. (2007). Considering the Problem of Insider IT Misuse. *Australasian Journal of Information Systems, 10*(2). doi:10.3127/ajis.v10i2.160

Garrett, C. (2004). Developing a Security-Awareness Culture - Improving Security Decision Making. Retrieved November 29, 2011, from http://www.eisf.eu/resources/item.asp?d=4832

Gerber, & Vonsolms, R. (2005). Management of risk in the information age. *Computers Security, 24*(1), 16–30. doi:10.1016/j.cose.2004.11.002

Gillespie, D. F., & Streeter, C. (1987). Conceptualizing and measuring disaster preparedness. *International journal of Mass Emergencies and Disasters, 5*(2), 155–176.

Goldsborough, R. (2007). How Serious a Threat Are Computer Viruses? *Tech Directions, 67*(1), 14. doi:Article

Goodman, J., Cormack, G. V., & Heckerman, D. (2007). Spam and the ongoing battle for the inbox. *Communications of the ACM, 50*(2), 24–33. doi:10.1145/1216016.1216017

Gray, C. D., & Kinnear, P. R. (2011). *IBM SPSS Statistics 19 Made Simple*. Psychology Press.

Greening, D., & Johnson, R. (1996). Do Managers and Strategies Matter? A Study In Crisis. *Journal of Management Studies, 33*(1), 25–51.

Gregor, S. (2006). The Nature of Theory in Information Systems. *Management Information Systems Quarterly*, *30*(3). Retrieved from http://aisel.aisnet.org/misq/vol30/iss3/5

Guba, E., & Lincoln, Y. (1994). Major paradigms and perspectives. In N. K. Denzin & Y. S. Lincoln (Eds.), *The SAGE Handbook of Qualitative Research* (Eds., pp. 105–117). SAGE.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1995). *Multivariate Data Analysis: With Readings*. Prentice Hall.

Hanson, W. E., Creswell, J. W., Plano Clark, V. L., Petska, K. S., & Creswell, J. D. (2005). Mixed Methods Research Designs in Counseling Psychology. *Journal of Counseling Psychology*, *52*(2), 224–235. doi:37/0022-0167.52.2.224

Hart, P., Heyse, L., & Boin, A. (2001). New Trends in Crisis Management Practice and Crisis Management Research: Setting the Agenda. *Journal of Contingencies and Crisis Management*, *9*(4), 181–188. doi:10.1111/1468-5973.00168

Helms, J. E., Henze, K. T., Sass, T. L., & Mifsud, V. A. (2006). Treating Cronbach's Alpha Reliability Coefficients as Data in Counseling Research. *The Counseling Psychologist*, *34*(5), 630 –660. doi:10.1177/0011000006288308

Herrmann, D. S. (2007). *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI* (1st ed.). Auerbach Publications.

Hinkin, T. R. (1998). A Brief Tutorial on the Development of Measures for Use in Survey Questionnaires. *Organizational Research Methods*, *1*(1), 104–121. doi:10.1177/109442819800100106

Hirschheim, R. (1992). Information Systems Epistemology: An Historical Perspective. Retrieved June 29, 2011, from http://areadocenti.eco.unicas.it/virili/TerracinaRW/Kit/HirschheimISEpistemology.pdf

Hough, M. (2005). Crisis Planning: Increasing effectiveness, decreasing discomfort. *Journal of Business and Economics research*, *3*(4).

Hu, Q., Hart, P., & Cooke, D. (2006). The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective, *6*(C), 127a. doi:10.1109/HICSS.2006.481

Hwacha, V. (2005). Canada'S Experience In Developing A National Disaster Mitigation Strategy: A Deliberative Dialogue Approach. *Mitigation and Adaptation Strategies for Global Change*, *10*(3), 507–523.

International Organization for Standardization. (2005). ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements. Text. Retrieved February 17, 2012, from http://www.iso.org/iso/catalogue_detail?csnumber=42103

Jain, A., & Singh, A. K. (2012). Distributed Denial of Service Attacks - Classification and Implications. *Journal of Information and Operations Management*, *3*(1), 136–140.

Jaques, T. (2010). Embedding issue management as a strategic element of crisis prevention. *Disaster Prevention and Management*, *19*(4), 469–482. doi:10.1108/09653561011070385

Jarvenpaa, S. L., & Staples, D. S. (2001). Exploring perceptions of organizational ownership of information and expertise. *Journal of Management Information Systems*, *18*(1), 151–183.

Jasanoff, S. (1993). Crisis Management: Bridging the Two Cultures of Risk Analysis1,2. (A. Boin, Ed.)*Sage Publications*, *II*(2), 123–129. doi:10.1111/j.1539-6924.1993.tb01057.x

Jensen, T. B., Kjærgaard, A., & Svejvig, P. (2009). Using institutional theory with sensemaking theory: A case study of information system implementation in

healthcare. *Journal of Information Technology*, *24*(4), 343–353. doi:10.1057/jit.2009.11
Jones, A. (2007). A Framework for the Management of Information Security Risks. *BT Technology Journal*, *25*(1), 30–36. doi:10.1007/s10550-007-0005-9
Jordan, E. (1999). IT contingency planning: management roles. *Information Management & Computer Security*, *7*(5), 232.
Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods information systems research: A case study. *Management Information Systems Quarterly*, *12*(4), 571–586. doi:10.2307/249133
Kim, Y., Cha, H., & Kim, J. R. (2008). Developing a Crisis Management Index: Applications in South Korea. *Journal of Public Relations Research*, *20*(3), 328. doi:10.1080/10627260801962962
Klassen, R. D., & Jacobs, J. (2001). Experimental comparison of Web, electronic and mail survey technologies in operations management. *Journal of Operations Management*, *19*(6), 713–728. doi:16/S0272-6963(01)00071-7
Kuhn, D. R. (1997). Sources of failure in the public switched telephone network. *Computer*, *30*(4), 31–36. doi:10.1109/2.585151
Kumar, S., & Gomez, O. (2010). Denial of Service Due to Direct and Indirect ARP Storm Attacks in LAN Environment. *Journal of Information Security*, *1*(2), 88–94.
Kusumasari, B., Alam, Q., & Siddiqui, K. (2010). Resource capability for local government in managing disaster. *Disaster Prevention and Management*, *19*(4), 438.
Landry, M., & Banville, C. (1992). A disciplined methodological pluralism for MIS research. *Accounting, Management and Information Technologies*, *2*(2), 77–97. doi:16/0959-8022(92)90002-A
Leidner, D. E., Pan, G., & Pan, S. L. (2009). The role of IT in crisis response: Lessons from the SARS and Asian Tsunami disasters. *The Journal of Strategic Information Systems*, *18*(2), 80–99. doi:doi: DOI: 10.1016/j.jsis.2009.05.001
Lettieri, E., Masella, C., & Radaelli, G. (2009). Disaster management: Findings from a systematic review. *Disaster Prevention and Management*, *18*(2), 117.
Lewis, B. R., Templeton, G. F., & Byrd, T. A. (2005). A methodology for construct development in MIS research. *European Journal of Information Systems*, *14*(4), 388–400. doi:10.1057/palgrave.ejis.3000552
Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. SAGE.
Lippert, S. K., & Volkmar, J. A. (2007). Cultural aspects on technology performance and utilization: A comparison of U.S. and Canadian users. *Journal of Global Information Management*, *15*(2), 56+.
Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. doi:10.1016/0022-1031(83)90023-9
Magklaras, G. ., & Furnell, S. . (2001). Insider Threat Prediction Tool: Evaluating the probability of IT misuse. *Computers & Security*, *21*(1), 62–73. doi:10.1016/S0167-4048(02)00109-8
Mansor, S., Shariah, M. A., Billa, L., Setiawan, I., & Jabar, F. (2004). Spatial technology for natural risk management. *Disaster Prevention and Management: An International Journal*, *13*(5), 364–373.
Markoff, J. (2009). Defying Experts, Rogue Computer Code Still Lurks. *The New York Times*. Retrieved from http://www.nytimes.com/2009/08/27/technology/27compute.html
Mayer, B. W., Moss, J., & Dale, K. (2008). Disaster and Preparedness: Lessons from Hurricane Rita. *Journal of Contingencies and Crisis Management*, *16*(1), 14–23. doi:10.1111/j.1468-5973.2008.00531.x

Mingers, J. (2003). The paucity of multimethod research: A review of the information systems literature. *Information Systems Journal*, *13*(3), 233–249. doi:10.1046/j.1365-2575.2003.00143.x

Mithas, S., Ramasubbu, N., & Sambamurthy, V. (2011). How Information Management Capability Influences Firm Performance. *MIS Quarterly*, *35*(1), 237.

Mitroff, I. (2005). *Why Some Companies Emerge Stronger and Better from a Crisis: 7 Essential Lessons for Surviving Disaster* (1st ed.). AMACOM.

Mitroff, I. I. (2004). Think like a sociopath, act like a saint. *Journal of Business Strategy*, *25*(5), 42–53. doi:10.1108/02756660410558933

Mitroff, I., Pauchant, T., Finney, M., & Pearson, C. (1989). Do (some) organizations cause their own crises? The cultural profiles of crisis-prone vs. crisis-prepared organizations. *Organization & Environment*, *3*(4), 269 –283. doi:10.1177/108602668900300401

Morrow, S. L. (2007). Qualitative Research in Counseling Psychology. *The Counseling Psychologist*, *35*(2), 209 –235. doi:10.1177/0011000006286990

Mulilis, J.-P., & Lippa, R. (1990). Behavioral Change in Earthquake Preparedness Due to Negative Threat Appeals: A Test of Protection Motivation Theory. *Journal of Applied Social Psychology*, *20*(8), 619–638. doi:10.1111/j.1559-1816.1990.tb00429.x

Myers, M. (1997). Qualitative Research in Information Systems. *Management Information Systems Quarterly*, *21*(2). Retrieved from http://aisel.aisnet.org/misq/vol21/iss2/6

Nelson, C., Lurie, N., & Wasserman, J. (2007). Assessing Public Health Emergency Preparedness: Concepts, Tools, and Challenges. *Annual Review of Public Health*, *28*(1), 1–18. doi:10.1146/annurev.publhealth.28.021406.144054

Nelson, C., Lurie, N., Wasserman, J., & Zakowski, S. (2007). Conceptualizing and defining public health emergency preparedness. *American Journal of Public Health*, *97 Suppl 1*, S9–11. doi:10.2105/AJPH.2007.114496

Nelson, K. (2006). Examining Factors Associated with IT Disaster Preparedness. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006. HICSS '06* (Vol. 8, p. 205b– 205b). Presented at the Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006. HICSS '06, IEEE. doi:10.1109/HICSS.2006.166

New Zealand Statistics. (2010). Experienced ICT attack that resulted in loss. Retrieved August 3, 2012, from http://www.stats.govt.nz/~/media/Statistics/browse-categories/business/bus-growth-innovation/bus-operations-survey/BOS-april10-all-tables.xls

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory*. McGraw-Hill.

Omar, A., Alijani, D., & Mason, R. (2011). Information Technology Disaster Recovery Plan: Case Study. *Academy of Strategic Management Journal*, *10*(2), 127.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, *2*(1), 1 –28. doi:10.1287/isre.2.1.1

Östlund, U., Kidd, L., Wengström, Y., & Rowa-Dewar, N. (2011). Combining qualitative and quantitative research within mixed method research designs: A methodological review. *International Journal of Nursing Studies*, *48*(3), 369–383. doi:16/j.ijnurstu.2010.10.005

Pahnila, S., Siponen, M., & Mahmood, A. (2007a). Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. *PACIS 2007 Proceedings*. Retrieved from http://aisel.aisnet.org/pacis2007/73

Pahnila, S., Siponen, M., & Mahmood, A. (2007b). Employees' Behavior towards IS Security Policy Compliance. In *Proceedings of the 40th Annual Hawaii International*

Conference on System Sciences (p. 156b–). Washington, DC, USA: IEEE Computer Society. doi:10.1109/HICSS.2007.206

Parnell, J. A., Koseoglu, M. A., & Spillan, J. E. (2010). Crisis Readiness in Turkey and the United States. *Journal of Contingencies and Crisis Management*, *18*(2), 108–116. doi:10.1111/j.1468-5973.2010.00603.x

Pearson, C. M., & Clair, J. A. (1998). Reframing Crisis Management. *The Academy of Management Review*, *23*(1), 59–76.

Pearson, C., & Mitroff, I. (1993). From Crisis Prone to Crisis Prepared: A Framework for Crisis Management. *The Executive*, *7*(1), 48–59.

Pedhazur, E. J., & Schmelkin, L. P. (1991). *Measurement, design, and analysis: an integrated approach*. Routledge.

Perrow, C. (1999). *Normal Accidents: Living with High-Risk Technologies* (Updated.). Princeton University Press.

Pfleeger, S. L. (2000). Risky business: What we have yet to learn about risk management. *Journal of Systems and Software*, 265–273.

Pinsonneault, A., & Kraemer, K. L. (1993). Survey research methodology in management information systems: An assessment. *Journal of Management Information Systems*, *10*(2), 75.

Pinta, J. (2011). Disaster Recovery Planning as Part of Business Continuity Management. *AGRIS On-line Papers in Economics and Informatics*, *3*(4), 55–61.

Polkinghorne, D. E. (2005). Language and Meaning: Data Collection in Qualitative Research. *Journal of Counseling Psychology*, *52*(2), 137–145. doi:10.1037/0022-0167.52.2.137

Pollard, D., & Hotho, S. (2006). Crises, scenarios and the strategic management process. *Management Decision*, *44*(6), 721–736. doi:10.1108/00251740610673297

Ponterotto, J. G. (2005). Qualitative Research in Counseling Psychology: A Primer on Research Paradigms and Philosophy of Science. *Journal of Counseling Psychology*, *52*(2), 126–136. doi:10.1037/0022-0167.52.2.126

Porras, P. (2009). Inside Risks: Reflections on Conficker. *Association for Computing Machinery. Communications of the ACM*, *52*(10). Retrieved from http://search.proquest.com/pqcentral/docview/237057144/1385E98F03EFF3DF37/1?accountid=14782

Preble, J. F. (1997). Integrating the Crisis Management Perspective into the Strategic Management Process. *Journal of Management Studies*, *34*(5), 769–791. doi:10.1111/1467-6486.00071

Provos, N., McNamee, D., Mavrommatis, P., Wang, K., & Modadugu, N. (2007). The ghost in the browser analysis of web-based malware. In *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets* (pp. 4–4). Berkeley, CA, USA: USENIX Association. Retrieved from http://dl.acm.org.helicon.vuw.ac.nz/citation.cfm?id=1323128.1323132

Puhakainen, P. (2006). *A design theory for information security awareness.* Oulu, Finland. Retrieved from http://herkules.oulu.fi/isbn9514281144/

Quinn, S. (2010). New Zealand Computer Crime & Security Survey. *New Zealand Computer Crime and Security Survey*. Security. Retrieved July 31, 2012, from http://internetnz.net.nz/our-work/security/2010-new-zealand-computer-crime-security-survey

Racherla, P., & Hu, C. (2009). A Framework for Knowledge-Based Crisis Management in the Hospitality and Tourism Industry. *Cornell Hospitality Quarterly*, *50*(4), 561 –577. doi:10.1177/1938965509341633

Rainer, R. K., Snyder, C. A., & Houston H. Carr. (1991). Risk Analysis for Information Technology. *Journal of Management Information Systems*, *8*(1), 129–147.

Ravichandran, T., & Rai, A. (2000). Quality Management in Systems Development: An Organizational System Perspective. *MIS Quarterly*, *24*(3), 381. doi:10.2307/3250967
Reilly, A. H. (1993). Preparing for the worst: The process of effective crisis management. *Organization & Environment*, *7*(2), 115 –143. doi:10.1177/108602669300700204
Rhee, H., & Kim, C. (2005). I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security. *Information Systems Journal*.
Rich, D. (2007). Authentication in Transient Storage Device Attachments. *Computer*, *40*(4), 102 –104. doi:10.1109/MC.2007.116
Richardson, R. (2007). *Computer Crime and Security Survey*. Retrieved from http://www.newmedia.org/articles/2007-csifbi-computer-crime-and-security-survey.html
Richardson, R. (2008). *CSI Computer Crime & Security Survey*. Retrieved from http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf
Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of personality and social psychology*, *52*(3), 596–604.
Rippl, S. (2002). Cultural theory and risk perception: A proposal for a better measurement. *Journal of Risk Research*, *5*(2), 147–165. doi:10.1080/13669870110042598
Rivard, S., Raymond, L., & Verreault, D. (2006). Resource-based view and competitive strategy: An integrated model of the contribution of information technology to firm performance. *The Journal of Strategic Information Systems*, *15*(1), 29–50. doi:doi: DOI: 10.1016/j.jsis.2005.06.003
Robert, B., & Lajtha, C. (2002). A New Approach to Crisis Management. Retrieved October 11, 2010, from http://onlinelibrary.wiley.com/doi/10.1111/1468-5973.00195/abstract
Roberts, K. H. (1990). Some Characteristics of One Type of High Reliability Organization. *Organisation Science*, *1*(2), 160–176. doi:10.1287/orsc.1.2.160
Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, *91*(1), 93–114. doi:10.1080/00223980.1975.9915803
Romaniuk, J., Sharp, B., Paech, S., & Driesener, C. (2004). Brand and Advertising Awareness: A Replication and Extension of a Known Empirical Generalization, *12*(3). Retrieved from http://wwwdocs.fce.unsw.edu.au/marketing/amj_12_3_romaniuk_et_al.pdf
Rosenthal, U., & Kouzmin, A. (1997). Crises and Crisis Management: Toward Comprehensive Government Decision Making. *Journal of Public Administration Research and Theory: J-PART*, *7*(2), 277–304.
Rousaki, B., & Alcott, P. (2006). Exploring the crisis readiness perceptions of hotel managers in the UK. *Tourism and Hospitality Research*, *7*(1), 27–38. doi:10.1057/palgrave.thr.6050030
Sam, L. (2004). The Impact of IT Investment in RSA e-Commerce SME Organisations. *Electr Jour of Infor Syst Eval*, *7*(1), 49–59.
Savage, M. (2002). Business continuity planning. *Work Study*, *51*(5), 254–261. doi:10.1108/00438020210437277
Scott, J. E. (1995). The measurement of information systems effectiveness: Evaluating a measuring instrument. *ACM SIGMIS Database*, *26*(1), 43–61. doi:10.1145/206476.206484
Shaluf, I., Ahmadun, F., & Said, A. M. (2003). A review of disaster and crisis. *Disaster Prevention and Management*, *12*(1), 24–32. doi:10.1108/09653560310463829
Shaluf, M. (2008). Technological disaster stages and management. *Disaster Prevention and Management*, *17*(1), 114.

Sheppard, B. H., Jon Hartwick, & Warshaw, P. R. (1988). The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research. *Journal of Consumer Research*, *15*(3), 325–343.

Shrivastava, P. (1993). Crisis theory/practice: Towards a sustainable future. *Organization & Environment*, *7*(1), 23 –42. doi:10.1177/108602669300700103

Shrivastava, P. (1994). Technological and organizational roots of industrial crises: Lessons from Exxon Valdez and Bhopal. *Technological Forecasting and Social Change*, *45*(3), 237–253. doi:10.1016/0040-1625(94)90048-5

Shrivastava, P., Mitroff, I., Miller, D., & Miclani, A. (1988). Understanding Industrial Crises. *Journal of Management Studies*, *25*(4), 285–303. doi:10.1111/j.1467-6486.1988.tb00038.x

Simsek, Z., & Veiga, J. F. (2000). The Electronic Survey Technique: An Integration and Assessment. *Organizational Research Methods*, *3*(1), 93 –115. doi:10.1177/109442810031004

Sipior, J. C., & Ward, B. T. (2008). User perceptions of software with embedded spyware. *Journal of Enterprise Information Management*, *21*(1), 13–23. doi:http://dx.doi.org/10.1108/17410390810842228

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, *49*(8), 97–100. doi:10.1145/1145287.1145316

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' Adherence to Information Security Policies: An Empirical Study. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, & R. Solms (Eds.), *New Approaches for Security, Privacy and Trust in Complex Environments* (Vol. 232, pp. 133–144). Boston, MA: Springer US. Retrieved from http://link.springer.com/chapter/10.1007%2F978-0-387-72367-9_12?LI=true

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. doi:10.1108/09685220010371394

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *SIGMIS Database*, *38*(1), 60–80. doi:10.1145/1216218.1216224

Sivo, S. A., Saunders, C., Chang, Q., & Jiang, J. J. (2006). How Low Should You Go? Low Response Rates and the Validity of Inference in IS Questionnaire Research. *Journal of the Association for Information Systems*, *7*(6). Retrieved from http://aisel.aisnet.org/jais/vol7/iss6/17

Smaltz, D., Sambamurthy, V., & Agarwal, R. (2006). The Antecedents of CIO Role Effectiveness in Organizations: An Empirical Study in the Healthcare Sector. *IEEE Transactions on Engineering Management*, *53*(2), 207.

Smith, D. (2003). Major organisations take to managing risk - Computer Business Review Africa. Retrieved September 10, 2012, from http://cbr.co.za/news.aspx?pklnewsid=9626

Smith, S., & Jamieson, R. (2006). Determining Key Factors in E-government Information Systems Security. *Information Systems Management*, *23*(2), 23.

Smits, S. J., & Ally, N. E. (2003). "Thinking the Unthinkable" — Leadership's Role in Creating Behavioral Readiness for Crisis Management. *Competitiveness Review: An International Business Journal incorporating Journal of Global Competitiveness*, *13*(1), 1–23. doi:10.1108/eb046448

Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133.

Starbuck, W. H., & Milliken, F. J. (1988). Challenger: Fine-tuning the Odds Until Something Breaks. *Journal of Management Studies*, *25*(4), 319–340. doi:10.1111/j.1467-6486.1988.tb00040.x

Steiert, M. J. W. (2007). Disaster preparedness. *AORN Journal*, *86*(2), 175–176. doi:10.1016/j.aorn.2007.07.013

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Computer Security: Risk Management Guide for Infomation Technology Systems. National Institute of Standards and Technology, U.S Department of Commerce. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Straub, D., Boudreau, M., & Gefen, D. (2000). Structural Equation Modeling and Regression: Guidelines for Research Practice. *Communications of the Association for Information Systems*, *4*(1). Retrieved from http://aisel.aisnet.org/cais/vol4/iss1/7

Straub, D., Gefen, D., & Boudreau, M.-C. (2005). *Research in Information Systems: A handbook for research supervisors and their students*. (D. Avison & J. Pries-Heje, Eds.). Amsterdam: Butterworth-Heinemann.

Straub, D. W. (1989). Validating Instruments in MIS Research. *MIS Quarterly*, *13*(2), 147–169. doi:10.2307/248922

Susanto, L. (2003). Business Continuity / Disaster Recovery Planning. Retrieved November 28, 2011, from http://www.susanto.id.au/papers/bcdrp10102003.asp

Sylves, R. (2008). Public Managers, Volunteer Organizations, and Disasters. *Public Manager*, *37*(4), 76.

Symantec. (2012). Internet Security Threat Report. *Enterprise Security Response*. Retrieved July 31, 2012, from http://www.symantec.com/threatreport/

Tetmeyer, A., & Saiedian, H. (2010). Security Threats and Mitigating Risk for USB Devices. *IEEE Technology and Society Magazine*, *29*(4), 44–49. doi:http://dx.doi.org.helicon.vuw.ac.nz/10.1109/MTS.2010.939228

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, *24*(6), 472–484. doi:10.1016/j.cose.2005.05.002

Tootle, D. M. (2007). Disaster Recovery in Rural Communities: A Case From Louisiana. In *Paper Presented at the Annual Meeting of the Rural Sociological Society*. Seelbach Hilton Hotel, Louisville, Kentucky. Retrieved from http://www.allacademic.com/meta/p124535_index.html

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2006). Formulating Information Systems Risk Management Strategies Through Cultural Theory. *Information Management & Computer Security*, *14*(3), 198–217. doi:10.1108/09685220610670378

Turner, B. A. (1976). The Organizational and Interorganizational Development of Disasters. *Administrative Science Quarterly*, *21*(3), 378–397. doi:10.2307/2391850

Turner, B., & Pidgeon, N. (1997). *Man-Made Disasters, Second Edition* (2nd ed.). Butterworth-Heinemann.

UN/ISDR. (2002). Living with risk: A global review of disaster reduction initiatives. Geneva. Retrieved from www.adrc.asia/publications/LWR/LWR_pdf/index.pdf

United States Computer Emergency Readiness Team. (2010). *Cyber Threats to Mobile Devices* (No. Technical Information Paper-TIP-10-105-01). Retrieved from http://www.us-cert.gov/reading_room/TIP10-105-01.pdf

Unlu, A., Kapucu, N., & Sahin, B. (2010). Disaster and crisis management in Turkey: A need for a unified crisis management system. *Disaster Prevention and Management*, *19*(2), 155.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425–478.

Vijayan, J. (2006). IT Risks Rise On USB Drives. *Computerworld*, *40*(40), 1–56.
Wade, M., & Hulland, J. (2004). Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research. *MIS Quarterly*, *28*(1), 107–142.
Watson, R. (2007). *Information Systems*. University of Georgia: Global Text Project. Retrieved from http://globaltext.terry.uga.edu/userfiles/Information Systems.pdf
Weirich, D., & Sasse, M. A. (2001). Persuasive password security. In *CHI '01 Extended Abstracts on Human Factors in Computing Systems* (pp. 139–140). New York, NY, USA: ACM. doi:10.1145/634067.634152
Whitman, M., & Mattord, H. (2005). *Principles of information security* (2nd ed.). Boston Mass.: Thomson Course Technology.
Wood, C. C. (1995). The Charles Cresson Wood file. *Information Management & Computer Security*, *3*(4), 23–26. doi:10.1108/09685229510097278
Woon, I., Tan, G.-W., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. *ICIS 2005 Proceedings*. Retrieved from http://aisel.aisnet.org/icis2005/31
Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management & Computer Security*, *16*(5), 463–483. doi:http://dx.doi.org/10.1108/09685220810920549
Yee, K.-P. (2004). Aligning security and usability. *IEEE Security Privacy*, *2*(5), 48 –55. doi:10.1109/MSP.2004.64
Yuan, J., & Jang, S. (2008). The Effects of Quality and Satisfaction on Awareness and Behavioral Intentions: Exploring the Role of a Wine Festival. Retrieved February 5, 2012, from http://search.proquest.com.helicon.vuw.ac.nz/pqcentral/docview/217431427/134B0B2711E7232DCDC/1?accountid=14782

Appendices

Appendix A- Information Sheet

User Awareness of and Adherence to Crisis Preparedness of the Information Systems in New Zealand Organisations

Name of the researcher: Dennis Ishumi

Institution: School of Information Management, Victoria University of Wellington.

I am a Master of Commerce and Administration student in Information Systems at Victoria University of Wellington. As part of this degree I am undertaking a research project leading to a thesis. This research project has the potential to help organisations improve or enhance user awareness of, and adherence to, crisis preparedness of their Information Systems against potentially adverse circumstances. In the context of this research project, crisis preparedness of the information systems means a wide range of activities including management and prevention of potential information systems threats and risks within the organisation.

Thank you for taking part in this study. The web survey will take approximately 15 minutes to complete. Your participation in this study is completely voluntary and your responses will remain anonymous. Your responses cannot be matched to your identity and will be released only as aggregates grouped with other employees' responses.

However, you may choose to enter your contact details if you would like to receive a summary of the report findings. This information will not be linked to your survey responses in order to ensure anonymity. All responses will be kept in a password protected file on a secure server, and will be deleted permanently once the findings have been communicated to interested individuals.

You may withdraw prior to submitting your responses without consequences of any sort. To leave the study simply select a *disagree* button below. Once you have submitted your responses it is no longer possible to withdraw your data because your responses are entered into a non-identifiable data file. All material collected will be kept confidential. No other person apart from me and my supervisor, Dr Philip Calvert, will see the survey responses and we will not be able to identify who they came from. Survey responses will form the basis of my research but only aggregated data will be used in the written report. The thesis will be submitted for marking to the School of Information Management and deposited in the University Library. It is intended that one or more articles will be submitted for publication in scholarly journals. The survey responses will be destroyed two years after the end of the project.

If you have any questions or would like to receive further information about the project, please contact me at **dennis.ishumi@vuw.ac.nz** or my supervisor, Dr Philip Calvert, at philip.calvert@vuw.ac.nz, or at the School of Information Management, Victoria University of Wellington, P O Box 600, Wellington 6140, Phone 04 463 6629.

Dennis Ishumi Signed:

Appendix B- Survey Instrument

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

User Awareness of and Adherence to Crisis Preparedness of the Information Systems in New Zealand Organisations

K1 I have read and understood the above information sheet and am willing to participate in this study.

- I agree
- I disagree

If "I disagree" Is Selected, Skip To End of Survey

D1 Gender: Please indicate what describes you best.

- Male
- Female

D2 Age (Years):

- 18-30
- 31-45
- 46 or above

D3 Do you work in an information technology (IT) or information systems (IS) department?

- Yes
- No

D4 Please indicate the number of years worked in the organisation.

- < 1 Year
- 1-10 Years
- 11-20 Years
- > 21 Years

Crisis preparedness means a wide range of activities including management and prevention of potential information systems threats and risks within the organisation.

On the basis of this statement please answer the following questions below.
S2.1 Which of these statements do you think represent activities associated with crisis preparedness of the information systems. **Please check all that apply**.

- ☐ Establishment of plans that will facilitate immediate response to events affecting the information systems of the organisation
- ☐ Continuously managing risks by applying appropriate protection to reduce information systems vulnerability to potential attacks
- ☐ Selecting and implementing a combination of security measures through the identification, control, and mitigation of information systems related risks
- ☐ Putting in place procedures that can facilitate an organisation to restore its information systems and services after a significant large-scale interruption
- ☐ End-users sharing information about security, such as exchanging passwords on a regular basis

S2.2 Please list down any activity or activities apart from those listed above that are being practiced in your organisation with regard to crisis preparedness of the information systems.

S3.1 Crisis preparedness of the information systems is primarily the responsibility of a selected group of people.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S3.2 The primary responsibility for the crisis preparedness of the information systems in my organisation lies with the…

- Management team
- Board of Directors
- Information Technology (IT) or Information Systems (IS) department
- Business function units
- IT/IS vendor or supplier
- I don't know
- Other: Please indicate _____

S3.3 Crisis preparedness of information systems is mainly the responsibility of all employees within the organisation.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S3.4 Crisis preparedness of information systems is not an independent activity, rather it is incorporated into my day to day activities.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S3.5 Crisis preparedness of the information systems is an activity that I must perform separately to my daily duties.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S4.1 I am aware of all major potential crises that can negatively impact the information systems of this organisation.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S4.2 Information about potential crises that can hit the information systems of this organisation has been clearly communicated to all stakeholders.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S4.3 Some of the incidents listed below are potentially capable of causing significant damages to the information and information systems services that can lead to major crises events to an organisation . Please **check all** that apply to your organisation.

- ❑ Unauthorised internal system access
- ❑ Unauthorised external system access
- ❑ Unexpected system shutdown
- ❑ Natural disasters (e.g. Floods, Earthquakes)
- ❑ Fire breakout
- ❑ Non-compliance with organisational information security policies
- ❑ None of the above
- ❑ I don't know

S4.4 It is probable that my organisation will encounter some of the threats and risks common to information systems platforms.

- Yes
- No
- I don't know

S4.5 In the occurrence of a major disastrous event such as an earthquake, fire breakout or flooding, what will be your first reaction? Please check the best answer.

- Run for my safety
- Stop and think the best way to contain the situation
- Follow the laid down procedures to avoid further damages or death
- Do nothing
- I don't know

S5.1 Are you aware of any period(s) that the information systems of your organisation went through a crisis?

- Yes
- No

If you selected "Yes" please respond to S5.2, if "No", move on to S5.3

S5.2 If Yes, do you believe that crisis preparedness measures in your organisation have improved from the previous event?

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S5.3 How would you rate the level of crisis preparedness of your organisation with regard to potential IS threats and risks as compared to other organisations in the same sector?

- Below Average
- Average
- Above Average

S5.4 Crisis preparedness measures in my organisation will protect critical business processes from potential IS threats and risks.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S5.5 Measures for crisis preparedness of the information systems in my organisation are developed enough for the organisation to cope in crises situations.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S5.6 Do you think the implementation of the measures for crisis preparedness of the information systems requires full participation of all end-users within your organisation?

- Definitely yes
- Probably yes
- Maybe
- Probably not
- Definitely not

S5.7 The implementation of crisis preparedness measures requires all teams (e.g. Information Technology/Information Systems, Business units or Human Resources) and individuals to cooperate fully with each other.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S5.8 In the implementation of the measures for crisis preparedness of the information systems, collaboration between teams is not necessary.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S6.1 Crisis preparedness measures in my organisation are processes that allow organisational information systems platforms to continue operating in times of uncertainty with minimum interruptions.

- Strongly Disagree
- Disagree

- Neither Agree nor Disagree
- Agree
- Strongly Agree

S6.2 I believe measures for the crisis preparedness of the information systems in my organisation have been operationalised.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S6.3 In my organisation crisis preparedness processes and procedures are kept current.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S6.4 In my organisation crisis preparedness processes and procedures are reviewed every…

- 6 months
- 12 months
- 24 months
- 36 months
- Only when there is an incident
- Only when it is necessary

S7.1 Crisis preparedness training is conducted in the following intervals. **Select only one** -

- Once per year
- After every two years
- After every three years
- None of the above

S7.2 Crisis preparedness training is conducted during the induction (orientation) programme.

- Yes
- No

S7.3 Crisis preparedness training is conducted when a new crisis preparedness measure is being implemented in the organisation.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S7.4 I cannot recall any crisis preparedness training being conducted in my organisation.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

If "Strongly Agree" Is Selected, Then Skip To End of Block S7

S7.5 My crisis preparedness training involves crises simulation so that I know exactly what to do in times of crises.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S7.6 My crisis preparedness training is in line with assigned duties and tested responsibilities.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S7.7 My crisis preparedness training includes an introduction to available resources and tools to use in the event of a crisis.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S7.8 Crisis preparedness training and communication in my organisation provide for employees to know precisely their role(s) in the event of a crisis.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S7.9 Crisis preparedness training and communication has created a readiness for end-users to work together in crisis situations.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S8.1 Failure by end-users to perform correct measures to counteract potential crises events will lead to negative consequences to the information systems of the organisation.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S8.2 I think unexpected system shutdown as a result of non compliance with the measures of the crisis preparedness of the information systems is a serious issue for the organisation.

- Strongly Disagree
- Disagree
- Neither Agree nor Disagree
- Agree
- Strongly Agree

S9.1 Information security is one approach used by organisations to secure or protect critical business systems from unauthorised access that can lead to information systems threats and risks. If these new changes are introduced to replace the current setup, how would you react to them?

	Very Displeased	Displeased	Somewhat Displeased	Neutral	Somewhat Pleased	Pleased	Very Pleased
A requirement that you change your security password every 60 days	○	○	○	○	○	○	○
Your new security password must be eight characters long and must combine letters, symbols and figures	○	○	○	○	○	○	○
The system logs you off when you are idle for five minutes either working from your office or remotely	○	○	○	○	○	○	○

S9.2 The back up of information can prove useful in a post crisis situation especially the information generated at the individual level. If these are new crisis preparedness measures, how would you react to them?

	Very Displeased	Displeased	Somewhat Displeased	Neutral	Somewhat Pleased	Pleased	Very Pleased
Ensure complete back up of personally generated information at the end of every week	○	○	○	○	○	○	○
Conduct a trial run to retrieve backed up information after every six months	○	○	○	○	○	○	○

T1 ** Thank you so much for taking the time to complete this survey **

Your responses will allow participating organisations to gain a better understanding of the level of end-user awareness of and adherence to crisis preparedness of the information systems in their organisations and how that can be improved or enhanced based on the findings from this research project. If you have suggestions/recommendations that may improve this study in the near future, please write them down in the box provided below.

Appendix C- Research Items

Variable	Item Wording (Attitude Towards CPIS)
ATTC1	S3.3 Crisis preparedness of the information systems is mainly the responsibility of all employees within the organisation
ATTC2	S3.4 Crisis preparedness of the information systems is not an independent activity rather it is incorporated into my day to day activities
ATTC3	S3.5 Crisis preparedness of the information systems is an activity that I must perform separately to my daily duties
ATTC4	S5.6 Do you think the implementation of the measures for crisis preparedness of the information systems requires full participation of all end-users within your organisation?
ATTC5	S3.1 Crisis preparedness of the information systems is primarily the responsibility of a selected group of people

Variable	Item Wording (Normative Expectations)
NE1	S5.7 The implementation of crisis preparedness measures requires all teams (e.g. Information Technology/Information Systems, Business units or Human Resources) and individuals to cooperate fully with each other
NE2	S5.8 In the implementation of the measures for crisis preparedness of the information systems, collaboration between teams is not necessary
NE3	S7.8 Crisis preparedness training and communication in my organisation provide for employees to know precisely their role(s) in the event of a crisis
NE4	S7.9 Crisis preparedness training and communication has created a readiness for end-users to work together in crisis situations?

Variable	Item Wording (Intention to Comply)
ITC1	S4.5 In the occurrence of a major disastrous event such as an earthquake, fire breakout or flooding, what will be your first reaction?
ITC2	A requirement that you change your security password every 60 days
ITC3	Your new security password must be eight characters long and must combine letters, symbols and figures
ITC4	The system logs you off when you are idle for five minutes either working from your office or remotely
ITC5	Ensure complete back up of all personal generated information at the end of every week
ITC6	Conduct a trial run to retrieve backed up information after every six months

Variable	Item Wording (Threat Appraisal)
TA1	S4.4 It is probable that my organisation will encounter some of the threats and risks common to information systems platforms
TA2	S8.1 Failure by end users to perform correct measures to counteract potential crises events will lead to negative consequences to the information systems of the organisation
TA3	S8.2 I think unexpected system shutdown as a result of non compliance with the measures of the crisis preparedness of the information systems is a serious issue for the organisation
TA4	S8.3 Do you think the allowance to BRING YOUR OWN DEVICE (e.g. iPad, notebook) to work has any detrimental effects to the crisis preparedness of the information systems of your organisation?

Variable	Item Wording (Response Efficacy)
RE1	S5.2 If Yes, do you believe that crisis preparedness measures in your organisation have improved from the previous event?
RE2	S5.3 How would you rate the level of crisis preparedness of your organisation with regard to potential information systems threats and risks as compared to other organisations in the same sector?
RE3	S5.4 Crisis preparedness measures in my organisation will protect critical business processes from potential information systems threats and risks
RE4	S7.2 Crisis preparedness training is conducted during the induction (orientation) programme
RE5	S7.4 I cannot recall any crisis preparedness training being conducted in my organisation
RE6	S7.5 My crisis preparedness training involves crises simulation so that I know exactly what to do in times of crises
RE7	S7.7 My crisis preparedness training include introduction to available resources and tools to use in the event of a crisis

Variable	Item Wording (Self Efficacy)
SE1	S4.2 Information about potential crises that can hit the information systems of this organisation has been clearly communicated to all stakeholders
SE2	S5.5 Measures for crisis preparedness of the information systems in my organisation are developed enough for the organisation to cope in crises situations
SE3	S6.2 I believe measures for the crisis preparedness of the information systems in my organisation have been operationalised
SE4	S6.4 In my organisation crisis preparedness processes and procedures are reviewed every…
SE5	S7.1 Crisis preparedness training is conducted in the following intervals. Select only one
SE6	S7.3 Crisis preparedness training is conducted when a new crisis preparedness measure is being implemented in the organisation
SE7	S7.6 My crisis preparedness training are in-line with assigned duties and tested responsibilities

Variable	Item Wording (Crisis Preparedness Awareness)
CPA1	S2.1 Which of these statements do you think represent activities associated with crisis preparedness of the information systems. Please check all that apply.
CPA2	S2.2 Please list down any activity or activities apart from those listed above that are being practiced in your organisation with regard to crisis preparedness of the information systems
CPA3	S3.2 The primary responsibility for the crisis preparedness of the information systems in my organisation lies with the…
CPA4	S4.1 I am aware of all major potential crises that can negatively impact the information systems of this organisation
CPA5	S4.3 Some of the incidents listed below are potentially capable of causing significant damages to the information and information systems services that can lead to major crises events to an organisation . Please check all that apply to your organisation.
CPA6	S5.1 Are you aware of any period(s) that the information systems of your organisation went through a crisis?
CPA7	S6.1 Crisis preparedness measures in my organisation are processes that allow organisational information systems platforms to continue operating in times of uncertainty with minimum interruptions
CPA8	S6.3 In my organisation crisis preparedness processes and procedures are kept current

Appendix D- Multiple Response Items

Variable	Item Wording (Crisis Preparedness Awareness)
	Activities that represent Crisis preparedness of the information systems
CPA1.1	Does establishment of plans represent crisis preparedness?
CPA1.2	Does continuous managing of risks and threats represent crisis preparedness?
CPA1.3	Do identification, control and mitigation of security measures embrace crisis preparedness efforts?
CPA1.4	Do plans and procedures to facilitate restoration of affected systems represent crisis preparedness?
CPA1.5	Do end-users sharing information about security represent crisis preparedness?

Var.	Item Wording (Crisis Preparedness Awareness)
	Incidents that can lead significant damages to the information systems of the organisation
CPA5.1	Unauthorised internal system access
CPA5.2	Unauthorised external system access
CPA5.3	Unexpected system shutdown
CPA5.4	Natural disasters (e.g. Floods, Earthquakes)
CPA5.5	Fire breakout
CPA5.6	Non-compliance with organisational information security policies

Appendix C- Other Documentation

C.1 Human Ethics approval application form

SIM HUMAN ETHICS COMMITTEE

Application for Approval of Research Projects

Please email applications to your supervisor, who will then email it to a SIM HEC member for a preliminary review.

Note: The Human Ethics Committee attempts to have all applications approved within 6 working days, but a longer period may be necessary if applications require substantial revision.

1 NATURE OF PROPOSED RESEARCH:

(a) **Student Research**

(b) If Student Research Degree **MCA** Course Code **INFO 591**

(c) Project Title:

User Awareness of and Adherence to Crisis Preparedness of the Information Systems in New Zealand Organisations

2 INVESTIGATORS:

(a) Principal Investigator

Name: **Dennis Buberwa Ishumi**

E-mail address: **dennis.ishumi@vuw.ac.nz**

School/Dept/Group: **School of Information Management**

(b) Other Researchers

Name Position

…… ……..
…….. …….

(c) Supervisor (in the case of student research projects)

Dr. Philip Calvert Supervisor

3 DURATION OF RESEARCH

(a) Proposed starting date for data collection – **Soon after HEC approval is granted**. (Note: that NO part of the research requiring ethical approval may commence prior to approval being given)

(b)Proposed date of completion of project as a whole **March 2013**

4 PROPOSED SOURCE/S OF FUNDING AND OTHER ETHICAL CONSIDERATIONS

(a) Sources of funding for the project

Please indicate any ethical issues or conflicts of interest that may arise because of sources of funding e.g. restrictions on publication of results

Conflict of interest is unanticipated as there is no any external funding involved.

(b) Is any professional code of ethics to be followed **N**

(c) Is ethical approval required from any other body **N**

5 DETAILS OF PROJECT

Briefly Outline:

(a) The objectives of the project/research include:

i. **To determine the extent of end-user awareness within the organisation of the crisis preparedness of the information systems;**

ii. **To determine the extent of end-user adherence to the crisis preparedness of the information systems.**

(b) Method of data collection

This study will make use of a survey instrument to be distributed to the respondents through their email addresses. The email content will include the survey link and the information to access it. The survey process uses Qualtrics software and will be strictly anonymous. It is anticipated that it will take approximately 15 minutes to complete the survey. It is proposed to distribute the survey to the respondents soon after HEC approval is granted and three weeks later a follow up email will be sent as a reminder.

(c) The benefits and scientific value of the project

The primary value of this research to academia will be the expansion of the existing discourses on crisis-preparedness. This will be done by the application of existing theory to analyse the collected data. The consolidation of the theoretical

frameworks and the application of the theory to analyse data will add knowledge to the field of crisis preparedness in IS.

This study also offers value to the participating organisations. The significance of the results from this study will allow these organisations to gain a better understanding of the level of end-user awareness of and adherence to crisis preparedness of the information systems in their organisations. From this understanding organisations will be able to improve or enhance user participation in crisis preparedness of the information systems at all levels.

(d) Characteristics of the participants

- **The selected participants must be people employed by the organisation and perform their duties using workstation computers or laptops connected to the enterprise network**
- **They must have minimum knowledge in Information Systems and services offered over its platform**
- **They must have an official email address that will be used to access the web survey.**

(e) Method of recruitment

Two or three organisations will be approached to see if they are willing to support the research. When an organisation agrees, an IS manager will be asked to arrange for the distribution of the email message containing the link to the survey to all staff who fit the profile in 5 (d).

Participants in the study will be recruited from organisational employees who have access to (or use) information and information systems services from their workstation computers or laptops connected to the enterprise network. In other words, this is a group of people who use organisational information systems to carry out their daily duties.

(f) Payments that are to be made/expenses to be reimbursed to participants

None

(g) Other assistance (e.g. meals, transport) that is to be given to participants

None

(h) Any special hazards and/or inconvenience (including deception) that participants will encounter

None

(i) State whether consent is for: (Please indicate as many as it applies)

(i) the collection of data	**Y**
(ii) attribution of opinions or information	**N**
(iii) release of data to others	**N**

(iv) use for a conference report or a publication **Y**
(v) use for some particular purpose (specify) **N**

Attach a copy of any questionnaire or interview schedule to the application

(j) How is informed consent to be obtained (see paragraphs 4.31(g), 5.2, 5.5 and 5.61 of the Guidelines)

(i) the research is strictly anonymous, an information sheet is supplied and informed consent is implied by voluntary participation in filling out a questionnaire for example (include a copy of the information sheet) **Y**
(ii) the research is not anonymous but is confidential and informed consent will be obtained through a signed consent form (include a copy of the consent form and information sheet) **N**
(iii) the research is neither anonymous nor confidential and informed consent will be obtained through a signed consent form (include a copy of the consent form and information sheet) **N**
(iv) informed consent will be obtained by some other method (please specify and provide details) **N**

……..
.

With the exception of anonymous research as in (i), if it is proposed that written consent will not be obtained, please explain why

……..
.

(k)If the research will not be conducted on a strictly anonymous basis state how issues of confidentiality of participants are to be ensured if this is intended. (See paragraph 4.3.1(e) of the Guidelines). (e.g. who will listen to tapes, see questionnaires or have access to data). Please ensure that you distinguish clearly between anonymity and confidentiality. Indicate which of these are applicable.

(i) access to the research data will be restricted to the investigator **N**
(ii) access to the research data will be restricted to the investigator and their supervisor (student research) **Y**
(iii) all opinions and data will be reported in aggregated form in such a way that individual persons or organisations are not identifiable **Y**
(iv) Other (please specify)

(l) Procedure for the storage of, access to and disposal of data, both during and at the conclusion of the research. (see section 7 of the guidelines). Indicate which are applicable:

(i) all written material (questionnaires, interview notes, etc) will be kept in a locked file and access is restricted to the investigator Y

(ii) all electronic information will be kept in a password-protected file and access will be restricted to the investigator **Y**

(iii) all questionnaires, interview notes and similar materials will be destroyed:
(a) at the conclusion of the research **N**

or (b) **Two** years after the conclusion of the research **Y**

(iv) any audio or video recordings will be returned to participants and/or electronically wiped **N**

(v) other procedures (please specify):

……...

If data and material are not to be destroyed please indicate why and the procedures envisaged for ongoing storage and security

……...

(m) Feedback procedures (See section 8 of the Guidelines). You should indicate whether feedback will be provided to participants and in what form. If feedback will not be given, indicate the reasons why.

At the end of the study a 2 – 3 page summary version of the research report will be sent to participants using a mailing list which will be created as a secondary component of the survey. The Qualtrics software application allows participants who are interested in receiving a copy of the report findings of this study to be directed to a different web link in order to maintain anonymity during this study. This web link is configured so that respondents can provide their contact details without being linked to their survey responses. A full final report will be written based on the overall results from the study. One copy of the final report will be submitted to the management of the participating organisations for them to consider any recommendations /suggestions made by the researcher.

(n) Reporting and publication of results. Please indicate which of the following are appropriate. The proposed form of publications should be indicated on the information sheet and/or consent form.

(i) publication in academic or professional journals **Y**

(ii) dissemination at academic or professional conferences **Y**

(iii) deposit of the research paper or thesis in the University Library (student research) **Y**

(iv) a case study used for teaching purposes **N**

(v) other (please specify)

……...

Signature of investigators as listed on page 1 **(including supervisors) and Chair of SIM HEC.**

NB: <u>All investigators and the Chair of SIM HEC must sign the form, then send it to the SIM HEC administrator for filing once the electronic application has been approved.</u>

Dennis Buberwa Ishumi Date……...

Supervisor:

Dr. Philip Calvert Date……...

Chair of SIM HEC:

……. Date ……..

APPLICATIONS FOR HUMAN ETHICS APPROVAL

CHECKLIST

✓ Have you read the Human Ethics Committee Policy?

✓ Have you read the Faculty of Commerce and Administration's HEC Guide?

✓ Is ethical approval required for your project?

✓ Have you established whether informed consent needs to be obtained for your project?

✓ In the case of student projects, have you consulted your supervisor about any human ethics implications of your research?

✓ Have you included an information sheet for participants which explains the nature and purpose of your research, the proposed use of the material collected, who will have access to it, whether the data will be kept confidential to you, how anonymity or confidentiality is to be guaranteed?

☐ Have you included a written consent form?

✓ If not, have you explained on the application form why you do not need to get written consent?

Are you asking participants to give consent to:

- ✓ collect data from them
  - ☐ attribute information to them
  - ☐ release that information to others
- ✓ use the data for particular purposes

✓ Have you indicated clearly to participants on the information sheet and/or consent form how they will be able to get feedback on the research from you (e.g. they may tick a box on the consent form indicating that they would like to be sent a summary), and how the data will be stored or disposed of at the conclusion of the research?

✓ Have you included a copy of any questionnaire or interview checklist you propose using?

POINTERS TO AVOID HAVING APPLICATIONS RETURNED BEFORE HEC REVIEW

- **The approval process is speeded up by not requiring the hard copy of your application form with the signatures on it at the initial review process. The <u>complete</u> application (HEC application form, info sheet, consent form, covering letter, questionnaire etc.) is to be emailed as an attachment in one file to your supervisor who will email it to an SIM HEC member for a preliminary review.**
- Do not insert a date into item 3 a.
- Delete the "Y" or "N" option that is not required. **<u>DO NOT</u>** remove any other text from the application form.
- **BOLD** your answers if you wish but do not alter the font anywhere else in the form.

C.2 First Contact Email Template

Dear Colleague,

We are writing in advance to let you know that a few days from now you will receive in your email inbox a request to fill out a web survey for an important research study. This study is being conducted in collaboration with the School of Information Management at the Victoria University of Wellington.

This email is to let you know that you been chosen to participate in our study. The research study is designed to capture the degree to which people (end users) within the organisation are aware of and adhere to different measures of the crisis preparedness of the information systems.

Your participation in our study is highly appreciated. We thank you in advance for your time and consideration of this email.
Sincerely,

Dennis Ishumi
School of Information Management

C.3 Second Contact Email Template

Dear Respondent,

We'd like to invite you to take part in today's study about **Crisis preparedness of the information systems in New Zealand Organisations**.

It should take approximately **10 minutes** depending on your answers to complete this survey. We hope you find it interesting!

So that your views can be included we need you to finish the survey in the next **three weeks**. This survey will close when the three weeks lapse.

Your answers, your organisation and your identity are **completely anonymous**. Your views will be grouped with those of others so that individual people and their answers cannot be identified. All collected information will be kept in a password **protected file on a secure server** accessible only to me and my supervisor.

To start, just click on the link below. If you need to, you can stop the survey at any time on the way through and return to the same point at a later date (i.e. you can do it in small bits).

Please click here to take a survey.

Thanks, in advance, for your time and your views!

Dennis Ishumi
School of Information Management

C.4 Email Reminder Template

Dear Respondent,

About three weeks ago I sent a web-based survey to you that asked about your perception on **Crisis preparedness of the information systems in New Zealand Organisations**. Our records show that some of you have responded to our request by completing the survey, some are in progress and others have not started yet.

The point of views of people who have already responded have communicated a wide variety of ways in which they believe their organisation is prepared and how they see their role in the whole process of crisis preparedness of the information systems. We think the results are going to be very useful to all participating organisations and to the wider community of private and public organisations.

We are writing again because of the importance that your response has for helping to get credible results. Although we sent invitations to many other employees at Meridian Energy, it is only by hearing from nearly everyone in the sample that we can be sure that the results are truly representative. You have three more weeks to take the survey.

We hope that you will access the web-based survey and fill it out as soon as you can or you can do it now: **Please click here to take a survey.** But if for any reason you prefer not to participate in the study just ignore this reminder.

Thanks again for your time and your views!

Dennis Ishumi
dennis.ishumi@vuw.ac.nz

*C.5 **The Data Collection Process***

To Whom It May Concern,

This document gives you detailed explanation of the data collection process if your organisation agrees to participate into the study. All of the work will be done by me with a little assistance from the IT staff particularly on broadcasting the email message.
I promise this study will not be disruptive in any way to either IT staff or other employees. The survey is designed to ensure that the respondents will use approximate **10 minutes** or **less** of their time to fill out the questionnaire. We would also hope that (*organisation name*) will benefit from the results of the survey, giving you something back in return for the staff time given to us.

The process will go as follows:

1. An email template below will be sent to **IT staff** (or communication people) so that the same can be broadcasted to (organisation name) employees. This will be the first task IT staff will be helping us with.

First Contact Email

Dear Colleague,

We are writing in advance to let you know that a few days from now you will receive in your email inbox a request to fill out a web survey for an important research study. This study is being conducted in collaboration with the School of Information Management at the Victoria University of Wellington.

This email is to let you know that you been chosen to participate in our study. The research study is designed to capture the degree to which people (end users) within the organisation are aware of and adhere to different measures of the crisis preparedness of the information systems.

Your participation in our study is highly appreciated. We thank you in advance for your time and consideration of this email.
Sincerely,

Dennis Ishumi
School of Information Management

---

2. A second email template (see below) containing the survey link will also be sent to IT staff so that the same can be broadcasted to (organisation name) employees. This will be the second task we are asking a support from IT staff.

An email containing the survey link (*this will be sent two days later after the first one)*

Dear Respondent,

We'd like to invite you to take part in today's study about Crisis preparedness of the information systems in New Zealand Organisations.

It should take approximately 10 minutes depending on your answers to complete this survey. We hope you find it interesting!

So that your views can be included we need you to finish the survey in the next three weeks. This survey will close when the three weeks lapse.

Your answers are completely anonymous. Your views will be grouped with those of others so that individual people and their answers cannot be identified.

To start, just click on the link below. If you need to, you can stop the survey at any time on the way through and return to the same point at a later date.

Please click here to take a survey.

Thanks, in advance, for your time and your views!

Dennis Ishumi

If you would like to contact us about this survey, simply email us at dennis.ishumi@vuw.ac.nz

---

3. Once the employees fill out the questionnaire, their responses will automatically be sent to a designated server on our side. This means no one at (organisation name) will be responsible for managing the filled out questionnaires.

4. After three weeks I may ask IT staff to send out an email reminder to those who received the first invitation to ensure that they use this opportunity to participate if they have not done so.

5. A few months later a draft copy of the final report will be sent to **Communication department** to review the company narration.

6. At the end of the study a copy of the final report will be submitted to (organisation name). The report will contain the study finding, suggestions and recommendations which may be used for improvements or enhancements of user participation in crisis preparedness of the information systems at (organisation name).