INFORMATION TECHNOLOGY DISASTER RECOVERY AND BUSINESS CONTINUITY AT UNITED NATIONS OFFICE IN NAIROBI, KENYA

BENJAMIN O. AKWAH

D61/ 75095/2014

A MANAGEMENT RESEARCH PROJECT SUBMTTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

OCTOBER, 2016

DECLARATION

This is my original work and it has not been presented in any other university for an award of a degree in any university.

Signed:……. Date……

BENJAMIN OPIYO AKWAH

D61/ 75095/2014

Supervisor's Declaration

The project has been approved with my authority as University supervisor

Dr. Kate Litondo

Department of Management Science,

School of Business

University of Nairobi

ACKNOWLEDGEMENT

This research project was a success because of the input by a few groups and people whom I want to acknowledge. My supervisor, Dr. Kate Litondo; who sacrificed her time to guide, direct me through the research process, United Nations Office in Nairobi, for assisting me in data collection. Finally, I wish to thank Almighty God for his love and blessings that kept me going.

DEDICATION

The research project is consecrated to my family, wife, children and friends for their love and support in several ways.

ABSTRACT

Organizations operate in an environment that is uncertain and unpredictable in estimating the nature, time and the magnitude of disruptions that might arise. It has therefore become important for the organizations to consider adopting a proactive approach in dealing with the uncertainty by developing a support framework to protect themselves against the outcomes of the disruptive events. The study was guided by the following objectives: To establish the extent to which United Nation has implemented IT disaster recovery plan. To establish the effect of disaster recovery on business continuity at the United Nation office in Nairobi and to determine the challenges of implementing disaster recovery. The research design adopted was descriptive research design. The study used primary data which was collected using questionnaires. The target respondents for the study were from the Finance, Human Resource and IT departments. These are the perceived technical people that were better placed to answer the research questions. In each department, 10 questionnaires were distributed. The data collected was analyzed using descriptive statistics including tables, pie- charts, percentages, mean and standard deviation. It was found that the organization recognizes the danger on its operations as a result of disasters occurring. Majority of respondents seemed to embrace almost all the steps in the various sections of BC and DR planning. Disaster management planning should involve all the stakeholders in a firm and at the same time be holistic in the sense that it should be strategic, consider business risk management analysis, awareness and Information Life cycle managements for the development of a business continuity plan. The model adopted for the study was found to be reliable. Back-up strategies and other undocumented back-up strategies were found to be statistically insignificant even though development of a plan, risk assessment and choosing an alternative recovery site were insignificant. The major limitation for the study was scope. The findings cannot be over generalized. The study was undertaken at United Nation Offices in Nairobi and therefore there's no room for comparison of findings with other offices. This study was also limited by other factors in that some respondents may have been biased or dishonest in their answers considering that they were all commenting on their employer. The study recommends there is need to enhance the organizational disaster recovery which will assist in the reduction of performance risk assessment. Disaster recovery helps the organization in tailored recovery plan that provide direction on how quickly to resolve the site issue. The study also recommends that there is need to manage on the organization conflict of interest among influential stakeholders, lack of clear policy guidelines and severity of disruptions. The study centered on disaster recovery principles and its effect on business continuity process in United Nation Office Nairobi. A similar study should therefore be done on other Parastatals in Kenya. This will shed more light on the disaster recovery principles and its effect on business continuity process in those Parastatals.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Changes emanating from environment are making firms to reconsider putting in place information systems which can handle the various risks facing information technology infrastructure. Process automation has computerized, manipulated, and analyzed business operations and long/short term strategies in a highly professional manner (Hiles, 2010). Indeed, it is difficult to envision contemporary businesses firm without advanced information systems covering their daily operations such as online trading and financial databases. However, with the increased dependence of the information system in the organizations operation, there has been increased risk of disasters occurring and with consequent disruptions of the firm's activities.

Businesses are prone to shock caused by disaster. Human losses and damage to properties, equipment; automobiles, and inventories are some of the direct impacts. The indirect effects include off-site business disruption, decline in property value and volatility at the stock market, portion of sociological and also environmental effects (Olshansky and Chang, 2009). Although many organizations are in agreement that a business continuity plan is critical to restore business operations in cases of disasters some firms lack appropriate plans in dealing with this kind of situations.

The growth and expansion in information systems at United Nation Office has contributed to a faster realization of the organizations objectives in an effective and efficient manner. At the United Nations Office in Nairobi, the organization's continuity is as a result of information system which acts as a strategic tool that enables its various departments that serves different countries in the region to deliver their services promptly (Swartz, 2003).

However in the application of the information systems, the medium are prone to cause disaster and unpredictable failures like data loss, virus infections, file loss, data center failures and network infrastructure breakdowns. In such a situation, disaster recovery plans come in handy in case of a risk occurrence. A disaster recovery plan is an aspect of a business continuity plan which includes processes, relevant procedures with policies which prepares a business for recovery in case disasters happen (Zobel and Khansa, 2014). Disaster recovery plans are a must for every organization and failure to plan is planning to fail. All firm's must be aware that they operate in risk environments that pose potential risks which if not properly mitigated can have adverse effects on a firm's operations hence the need for a BCP plan and proper disaster recovery plans embedded in them.

The current study is based on normative theories which provide frameworks to specify actions that need to be taken in relation to disasters. It comprises of comprehensive emergency management which stipulates common managerial functions in mitigation, preparedness, response, and recovery (Drabek, 2004). It suggests that an organisation is expected to choose the best mode that offers the highest risk-adjusted return on investment. This suggests that organisation need to develop disaster recovery plans and business continuity measures in restoring normalcy of operations after disasters have struck. The organisation need to identify the best recovery approach for all crucial business activities and services, set up a recovery management organization and make recovery strategies for various levels of business activities and services.

1.1.1 IT Disaster Recovery Process

Liu, Hwang, and Liu (2009) define disaster as disturbance or loss of essential service or procedures in an organization for a period of time making it impossible for the firm to achieve its mission and goals. Organisations can be affected by either of the following types of disasters; disasters caused by nature (natural catastrophes), disaster caused by technology (technological accidents) and those caused by actions of human beings. (Nolan, 2014) further defines disaster as unexpected happening that causes damages to the organization or put to a stop the organization functions. The course of action taken by an organization after disaster has struck is known as disaster recovery. All the actions, procedure undertaken by an organization to recuperate lost data, software and hardware required to go back in business after an event is known as disaster recovery (Slater, 2010). All the definitions above prove that disaster recovery is a strategic plan that an organization follows to resume back after disaster. Disaster recovery tries to reduce the loss taken by the firm and make an effort to resume the major functions.

1.1.2 Business Continuity

The capacity of a business to immediately go back to its usual activities after disaster is referred to as business continuity plan in Information Technology (Bajgoric, 2006).the process takes into consideration the major threats in relation to normal operations, identifies the major business process and the best strategies available to resume the organization functions. According to Slater (2010), disaster recovery can also be termed as business continuity plan that shows the organization behavior to handle likely disasters. Business continuity plan consists of actions and plans to resume major services and allows the organization to recuperate its facility and assets.

Business continuity plan clearly defines the process that the affected firm will use to resume back to operations. This plan also gives pointers on how to survive less catastrophic events (Altay and Green, 2006). Business continuity plan makes certain that business constancy is achieved by classifying the long term major strategies which are considered necessary. Firms are taking fundamental steps to ensure that their operations run smoothly without interferences that emanate from loss of data. In so doing, organisations are taking measures in ensuring they are ready for any form of disaster by all means.

1.1.3 United Nations Office in Nairobi

In 1996, the General Assembly established their UN headquarters office in Kenya. This office was mandated to serve as delegate of the UN secretary general in Africa. Under the leadership of a director general the office was commissioned to carry out representations ,connect UN functions with permanent missions, makes it easy for the United Nations Environment Programme (UNEP) and the United Nations Human Settlements Programme (UN-Habitat) to work together by offering administrative services; the office was also to give joint and common services to UN organization in Kenya as appropriate and lastly it was supposed to ensure United Nations Staff and assets are safe by giving security. UN office in Nairobi is a host to many UN Agencies that offer ICT infrastructure, internet connection through use of external ISP providers, LAN hosting and data center. This exposes the center to system attacks, power failures and disasters making UN relevant and ideal for this investigation. With the network infrastructure, shared and managed internet across other agencies, shared storage facility for servers and back up for all agencies, common managed telephone services, teleconferencing and video conferencing services. Sometimes they undergo outages and downtimes like power failures and fiber cuts.

This leads to unavailability of internet, cabling problems causing network failures and external system attacks that pose threats to data.

1.2 Research Problem

Organizations are increasingly subject to disruptions in their day-to-day operation and it has become unpredictable to estimate the nature, time and the magnitude of disruptions that might occur. Because of the increased uncertainty, it has become imperative for the organizations to adopt a proactive approach in dealing with the uncertainty and instead develop a support framework to protect themselves against the outcomes of the disruptive events (Wunnava, 2011). The intensity of disaster could be small or big but either can cause harm to business environment resulting to interruption of business work flow. A disaster can have a noteworthy, undeviating impact to a firm's capacity to keep on with business processing. These disruptions may be in form of the organizations inability to develop submissions or collect clinical trial data, delayed or limited ability to get information to the field or process sales data, or the inability to manufacture or communicate with the field offices in the case of the United Nations Office in Nairobi (Bajgori, 2006). Consequently, for effective information technology usage in organization there is need for the organization to have a disaster recovery mechanisms and business continuity plans to support business and ensure critical information is maintained without any loss.

Business continuity and preparing for a disaster gives firms such as UN a competitive gain because stakeholders will be able to be served better. The United Nations Office in Nairobi serves all United Nations agencies in Kenya and in the great lakes region and the number of beneficiaries, both internal and external, runs into tens of millions.

The ability to sustain time sensitive processes such as payroll to the staff and remittances of finances to different projects being financed by the UN affiliates will be hindered due to any disaster occurrence. Further, they may be unable to communicate internally or with customers, and there could be residual outcomes such as a lack of alignment with a parent company and partners, loss of worker productivity, or damaged credit rating from inability to pay bills. Consequently, if the problem is not addressed fast enough, The Company's reputation with customers, employees, partners, or other stakeholders may be damaged. Therefore, there is need for the United Nations Office in Nairobi to develop an appropriate disaster recovery and business continuity plan to avoid destruction of property, telecommunication providers' equipment, internet connectivity, land-line and mobile-communication networks.

A number of studies have been undertaken on the need for organizations to have an effective disaster recovery plan and its influence on the business continuity. Biswas and Choudhuri (2012) discovered that disaster recovery and business continuity plan is an essential component of the organization management plan. The importance of an effective disaster recovery and business continuity plan is regularly demonstrated in institutions which are strongly committed to their plans. Nyambura (2005) carried out a survey of ICT aspects of disaster recovery among companies quoted at the NSE.

He found that majority of the firms sampled did not have a functional plan that addresses all of the DR processes required to restore technology, but instead, disaster recovery was being taken as an auxiliary function without a defined owner responsible for maintenance of the plan on an ongoing basis.

Muoki (2010) who carried out a research on business continuity planning for a global business operator in less developed economies, a case study of General Motors East Africa. He found that business continuity measures are not well employed in the organization. Mathenge (2011) researched on the disaster recovery and business continuity plans in Class-A Parastatals in Kenya. He found that during pre-planning consulting business process owners was rendered to be a vital step during the business impact assessment. During plan development, developing a formal system backup policy and schedule was most important while during testing having frequently scheduled tests was most important. From the above studies, it is evident that the studies do not separate the two concepts of disaster recovery and business continuity. However, the present study sought to find out how organisation disaster recovery process impact on business continuation. A question was thus posed as: what is the influence of disaster recovery plan on business continuity at the United Nations Office in Nairobi, Kenya?

1.3 Research Objectives

The study was guided by the following objectives

a) To establish the extent to which United Nation has implemented IT disaster recovery plan.
b) To establish the effect of disaster recovery on business continuity at the United Nation office in Nairobi
c) To determine the challenges of implementing disaster recovery at United Nation Office in Nairobi

1.4 Value of the Study

The study outcome will be relevant to the United Nations offices and other organization in understanding the need for information technology in business

continuity and disaster recovery. The Management will be aware of the challenges faced in the adoption and implementation of business continuity and disaster recovery. The research will clearly depict how the United Nation organization must adapt recovery from a disaster and enhances continuation of a business.

This research will be of value to the government and regulatory agencies through findings and recommendations of this study useful in formulating business continuity and disaster recovery, policies and laws that will aid in regulating and operationalization of organisations in Kenya. Researchers might find this study resourceful in expounding their understanding on business continuity and appropriate ways to recover from a disaster. It can also be utilized as a basis for further research.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

Discussions have been provided in this chapter on the study variables, empirical studies that relate to the objectives and theories that give anchorage to this research.

2.2 Theoretical Foundation

In this section, discussed are the theories that give support to the study in relation to the variables under investigation. These theories are: Normal Accident and High Reliability. They have been discussed in light of the business interruptions and how firms should prepare to face disasters to continue with their operations normally.

2.2.1 Normal Accident Theory

The Normal Accident Theory (NAT) holds that organizational failure springs out from trying to make perfect organizations .NAT also clarifies how the technologies assumed by a firm can go hey wire .according to (Miller, 1998) views, the proficient and modern organization are more likely to produce disaster compared to the so not perfect organization. Lucid structures and process should be created and adopted by an organization to reduce or avert technologies possibilities. Although people have the abilities to create a faultless control mechanism this is partially impossible. (Smith, 2005) reveals that information and data gathering, processing and analysis cannot be a 100 percent accurate and sometimes the discrepancies are not observed right away this result to unintended costs. A significant principle of NAT is that these unplanned costs make use of the lucid organization to proliferate efficiently and quickly the lucid organization intended to manage disturbances, actually amplify errors and glitches, which can then spin out of control into disaster.

The theory tips out that errors are merely likely to extend into large-scale disasters if they take place in an organizational power hierarchy at a point at which they are likely to be exaggerated, and perhaps to be added among other less significant errors, via the process of the ordinary administrative processes (Turner and Pidgeon, 2007). The more interactively complex an organization is, the more its center technology and their interactions develop into, the harder it is for operators to understand the system and to get involved in an appropriate manner when the system acts in unexpected ways. Therefore, workers are bound to get the wrong idea about small problems and might set off corrective actions that stimulate rather than diminish the emerging disaster.

Shrivastava, Mitroff, Miller and Miglani (2008) opine that as Western societies become ever more complex and tightly coupled more breakdowns would be expected to occur, although this does not appear to be happening. However, this appears not to be the case and it can be argued that modern society has become safer. This theory therefore prompts such questions as; why do some organizations suffer normal breakdowns whereas many others do not? Could it be that some organizations have learnt to deal with complexity and tight coupling or have they found ways to discover emerging crises in time?

2.2.2 High Reliability Theory

This theory holds that there are certain factors that can aid an organisation to identify a forthcoming disaster through finding appropriate ways of making an earlier intervention (Weick & Sutcliffe, 2001). Firms are devising ways to ensure that their business run continuously without any form of interferences that might affect their performance. It is important to realize that a firm that has a pervasive culture of safety which draws awareness and preparation of an emergency.

Further, the firm should design mechanisms to enhance communication and alerts to help the organisation to easily detect disasters.

This expose the firm to understand how a disaster response might fail and what should be done to prevent such kind of eventualities. For an organisation to achieve reliability, it should have a track record to track a trail of events that might lead to disaster and establish efficient ways of managing such delicate situations (Egan, 2011).

The firm should work together as a team in curbing disasters. The IT departments should closely work with other departments through shared systems where all communication and decisions can be communicated and appropriate action taken. IT experts should embrace a culture of dynamism to support and implement changes that are essential in enabling the organisation to cope with technological changes that might weaken the systems and expose it to disasters (Perrow, 2006; Pfeffer, 1978; Schein, 1985). The top management should explain to the employees on the importance of having constant training and development programmes to enlighten them and expound their knowledge on information technology. This should be aligned with the technological changes and disaster recovery plans that guide the firm in putting effective measures which can accommodate nature of operations that might change from time to time (LaPorte, 2011; Rochlin, 2011). Employees are thus able to appreciate technological changes by coping with these changes, this makes them motivated to work efficiently, and overcome challenges avoid accidents and take correct measures in cases of disaster.

2.3 Disaster Recovery

Disaster Recovery according to (Birkmann, 2009) is an explanation of business response to unexpected internal or external disaster on how to resume all the major functions of a firm without obstructions. Birkmann also states that disaster recovery is normally associated with technology only and faces the recovery facility, operating systems, computer hardware, networking, and other infrastructure, application software, databases, and records. Glenn (2010) suggest use of logbooks, mobile phones and hardcopy documents in the recovery plan where technology is not available .To resume back normal business function a firm should have a disaster recovery strategy .this strategy plan should have a disaster detection, notification and coordination processes, communication strategies, alternate computing facilities management as well as disaster recovery plan testing and maintenance methods. Disaster recovery plan should be practicable dealing with all the processes necessary to resume technology. It should be assigned to a definite individual for continuance. When developing a disaster recovery plan the restoring should be done according to order of priority such that the major systems are recovered first. According to (Galindo and Batta, 2013) in case of an event that involves technology, one should ensure that network resumes first then applications afterwards. This is because applications are dependent of the network. After priority one should consider time required for the systems. The system which requires a 24/7 uptime should be considered first in relation to those that requires less attention. (Jackson, 2012) urges that developing a disaster recovery plan one needs to accumulate enough data on the technology basics in question, look at the conflicting priorities, the uptime and then determine the most suitable order of restoration. The selected order of restoration should be made available to the rest of system owners to avoid confusion.

DR operation competence necessary should be in relation to the business requirements (Losada, Scaparra and O'Hanley, 2012). A hot site is a network created purposely for recovering data in case of a disaster occurrence. A hot site is useful in case of a recovery plan involving speedy recovery of data and when the time given to resort a previous technology platform is not practicable. In the case of a hot site, the hardware needs to be previously at hand and mobile computing resources; where desk space for critical staff is available. The hot site is a service sort from service providers on contractual basis by the IT department

2.4 Challenges to Disaster Recovery Plans

Firms face several challenges from loss of information. Hager (2012) notes that poor planning by the firm by failure to identify systems that anchor the activities of organisations consisting of detailed plans of recovery to the initial position in cases of emergencies impacts negatively on the process of recovery. In most cases, people opt tend to assume that they understand their networks better while they know little about how they are configured and how these networks operate and more specifically how to effectively manage these systems to ensure that they perform optimally. Wallace and Webber (2012) observe that in cases where IT departments separates other departments making difficult to monitor the systems of other departments such that whenever a disaster struck it becomes a problem to detect and identify the cases of the problem. This causes delays and inefficiencies as the firm try to solve this problem leading to loss of important data and poor performance. The firm should design a strategy that allows the management team to have a disaster recovery plan before and after the occurrence of a disaster thus assisting the firm to handle disaster cases.

As Pitt and Goyal (2013) point out, the largest problem involving the top management is a lack of adequate level of support for full recovery, not conducting a business

impact analysis and addressing all gaps in your recovery model. Disaster recovery planning is becoming a prominent topic amongst most IT managers. This is due to the increased number of disasters whether through terrorist attacks or natural calamities, more and consequently, more and more boards are focusing on this issue (Losada, Scaparra, and O'Hanley, 2012). Many organizations now realize that indeed Kenya lies within the global arena and as such is affected by incidences like terrorist threats. With that realization, many organizations have DR and BC plans that encompass this kind of scenarios.

2.5 Business Continuity Plan

Cerullo & Cerullo (2004) defines business continuity planning as an element of (BCM) business continuity management procedure that recognizes probable risk, possibility and vulnerability and the impacts to an organization. According to (Cerullo, & Cerullo, 2004) BCM is a vital element of management especially when creating disaster recovery plans, this is because the BCM gives out methods and procedures for reducing risks and provide an efficient response to unsettling event in such a way that the organization status is maintained ,key stakeholders interest are preserved and profit maximization activities. Management process necessitate that BCM must be completely incorporated across the entire organization for it to be successful and feasible .The U.S. Federal Emergency Management Agency (FEMA) acknowledged the main objective of a business continuity plan as to lessen the outcome of any disruptive occurrence to a controllable level (FEMA, 2012). A company's task and functions, its competence, and its overall continuity strategy are the varying factors to the detailed objectives of any organizations continuity plan.

FEMA further states that continuity plans are intended for the following reasons; reduce injuries and loss of life, decrease property damage, alleviate the time, harshness of disruptions that are brought by the disaster, to plan the essential functions by order of priority and finally resume operations. Business continuity plan intends to safe guard organization records, assets and equipments and should be executable with or without warning. The period required to plan for sustainable continuity operations is thirty days or longer .this period is dependent on the organizations intangible and tangible assets, how different departments relate and the continuity plan adopted. Williamson (2002) maintains that one of the ways for an organization to enjoy continued existence and success lies in creating and sustaining a practicable business continuity plan (BCP). There are general principles regarding planning methodologies but some organization may differ in this. The subsequent are the five main steps in BC Planning:

2.5.1 Initiation

This is the initial meeting with senior management in the organization for without their support little, would be achieved in this regard. Some of the key steps in planning for this meeting include: Reviewing the organization to determine what resources are appropriate to be assigned to the project team. This involves reviewing any existing enterprise-wide disaster plans, policies, strategies and procedures relative to emergency response or continuity of operations. The other is review of any continuity plans that are in place within the organization and assess if they are effective models for the project. The third is research local events in the recent past such as fires, severe weather, major equipment failures, etc. that had or could have had a negative effect on the organization. The fourth is review any pertinent laws and regulations that may affect or hinder project.

The other is preparation of a project introduction Memo for senior management's signature to communicate to the organization at large, the need for BCP and the program's goals. Another step is preparation to discuss project funding by ensuring that management realizes that business continuity planning is an ongoing budget item, not a one-time project.

2.5.2 Business Impact Analysis (BIA)

Involves identification of the effects from disruption which affect the firm's approaches and techniques used to quantify and qualify such effects. Okolita (2009) notes that the process determines the things that needs to be recovered and speed at which this can be realized. This presumed to be a challenging task to execute which is considered very critical. The more time you have to bring a business function back in service following a disaster, the more your recovery options increase. The business impact analysis is invaluable for identifying what is at stake following a disaster and for justifying spending on protection and recovery capability. Nobody but you will mind.

Hiles (2003) states that, a Business Impact Analysis (BIA) involves identification of the magnitude of how the firm can get affected by risks in case it strikes. The business impact analysis process achieves several goals which include identifying financial and non-financial costs, establishing time window in which recovery takes place. Identifying materials required for recovery, making a preliminary examination of resources needed for recovery and provision of input to risk assessment on business related risks.

2.5.3 Disaster Readiness Strategies

Williamson (2002) identified the following as the strategies to include:

Define and Cost Business Continuity Alternatives- Using the information from the BIA, the project team should evaluate the alternative strategies that are available to the organization, narrow the list of alternatives to the two or three most plausible, and develop budgetary costs for each strategy. The resumption timeframes will play a significant role in determining which components may require prepositioning. Further, based on the, needs of the business and ones evaluation of alternatives, the project team should develop recommendations on which strategies to fund for implementation. Finally, there is need to prepare senior management report and presentation be made on the findings of the BIA, the strategy alternatives that were developed and investigated, and the project team's recommendation.

2.6 Empirical Studies on Disaster Recovery and Business Continuity

Firm's ability to cope with disaster situations depends highly on the preparations and the capability to counter calamites. Some of these factors include age, size, complexity and nature of the business (Rastegar and Khorram, 2014). Factors relating to disasters include human role, financial capacity, pre-disaster existing conditions among others, and their effect on businesses. The factors affect preparation, duration of interruption and retrieval. Tierney and Dahlhamer (2010) found that firms that face financial difficulties are unlikely to recover from loss of disaster caused by information technology. This is because such firms might not be in a position to make adequate preparations that can create a barrier in an IT linked disasters.

Organisations are highly exposed to disasters based on the resource capacity and the preparations that they make (Loscocco and Robinson, 2001). The resource base and capacity is instrumental in assisting the firm to counter exposure to calamities. Firms put in place protective measures based on the magnitude of the anticipated disaster.

Webb et al. (2009), holds that stable firms make huge investments in resources and trainings to ascertain employees are prepared and organized to face any eventuality rising from IT.

Mead and Liedholm (2008) notes that small firms are more exposed to loss of information since they lack finances to invest in shared systems that allow organisations to store data in the cloud.

This can also be attributed to poor governance and poor system administration due to lack of skills and access to information. Dahlhamer and Tierney (2010) assert that firms should have in place archives where access to information and maintenance can be made through efficient ways that allows a firm to save time. This information should be safeguarded to protect the future of the firm. Preparation is necessary and official communication is key to all stakeholders to ensure that it is exploited and utilized to serve organisational needs (Turner et al., 2006). Maintenance of systems and hardware should be done regularly to ensure that the environment is conducive for recovery of information (Danes et al., 2009)

Arminio and Truax (2005) showed relevance of Information Life Cycle Management on virtues of managing records. Notably, information preservation and making contingent plans are associated with preparation for emergencies which is a clear indication that firm's information is critical in the short-term particularly in making decisions. In support of this, Croy (2004) insists that information is power and should be utilized for the best interest of all the stakeholders. He adds that appropriate ways should be developed to avoid loss of information through proper storage mechanisms. Braverman (2006) notes that most crisis of disaster recovery was caused by human crisis affected negatively on the health and performance of employees.

This led to confusion which exposed the firm to disasters and loss of critical information while risking effective continuation of the business. Kirschenbaum (2006) found that firms that successful made relevant preparations were able to overcome problems that emanated from loss of data. This was achieved by ensuring that the organisation and the employees were aligned in recovering from disasters. The employees underwent training and were provided with the facilities to enable them to handle disasters.

2.7 Summary of the Literature

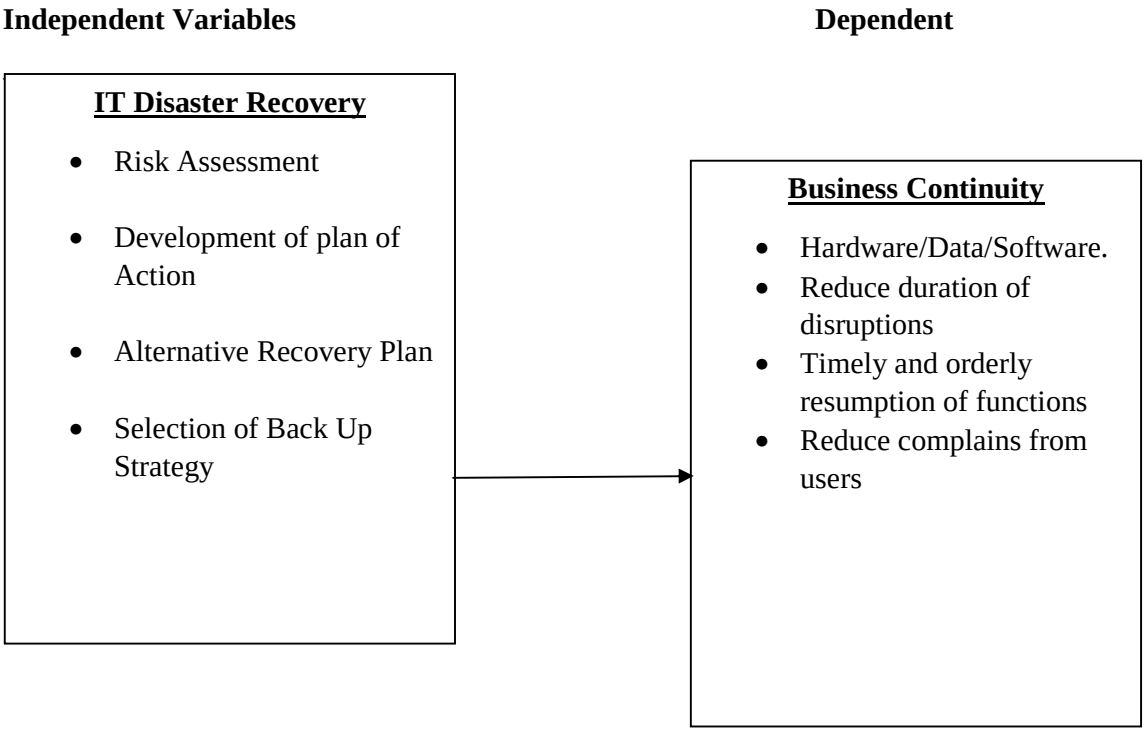
Influence of disaster recovery on the firm's business continuation has been conversed both in the literature and empirical findings. Firms have demonstrated the importance of recovering from IT related calamities and appropriate action that the top management should take to avoid such disasters. Organisations need to set up shared systems that can detect disaster at early stages thus aiding the organization to align itself and its employees to face any form of IT calamities. Firms should have a disaster plan to recover from disaster which should be communicated to all the employees. This can be realized through identifying, notifying, coordinating procedures, communicating including DR plan, testing and maintenance processes.

However, ability of the firm to develop ways of recovery from disasters varies from one organization to another. The uniqueness of the firms operations will determine the type of disaster recovery plans that need to be developed and the types of system support that has to be implemented in the organization. Due to this differentiation, the current research will look more on the application of Disaster recovery in the United Nations Office in Nairobi.

2.8 Conceptual Framework

A conceptual framework is set of ideas, put together to explain a given link between variables (Reichel and Ramey, 1987). It provides a diagrammatical presentation of a conceptual argument to aid the researcher to understand how IT disaster recovery of the firm affects continuity of a business.

Figure 2.1: Conceptual Model



Source: Researcher, 2016

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

Discussed in the chapter is the methodology which has been adapted to aid the researcher to address the objective of the study.

3.2 Research Design

The research design adopted was descriptive research design. According to Cooper and Schindler (2000), a descriptive research design is concerned with finding out the; who, what, where, when and how much. The design allows the study to test the link between disaster recovery and business continuity.

3.3 Population

A population includes the number of elements being studied. Additionally, Krishnaswami (2003) notes that a sample is drawn from a population whereby measures are taken. As per the UN office in Nairobi, HR employee data base, as at 30th June 2016, the number of management staff was 138 which formed the study population.

3.4 Data Collection

The study used raw sources of information. The choice of this data was informed by its convenience in collecting huge amounts of data in a short duration. With the questionnaire, it was easy for the researcher to assess attitude and perceptions of the respondents (Robson, 2002).

The questionnaire employed structured and open-ended questions to elicit responses for quantitative and qualitative analysis. A five points Likert Scale was implemented accordingly.

Part I one was used to answer objective one which was to establish the extent to which UN Office has implemented business continuity and disaster recovery. Part II helped to identify the challenges faced by the UN office in disaster recovery and the last part was to establish the effect of disaster recovery plan on business continuity process at the United Nations Office in Nairobi.

Target respondents were chosen from the Finance, Human Resource and IT departments. These were perceived to be technocrats and relevant in matters of IT. In each department, 10 questionnaires were distributed. Administration of questionnaires was executed by dropping and picking them later. Follow-ups were done to ascertain on-time gathering of data.

3.5 Data Analysis

Raw information was collated with the help of questionnaires. The output was produced in Tables and pie charts and measures summarized inform of standard deviation and mean. The analysis sought to meet the research objectives. Section one and two of the questionnaire which sought to answer the first two objectives and whose analysis was executed using descriptive statistics. The results were in a form of a table which showed mean and standard deviation of each of the respondent's performance measures. To establish relationships, a regression was implemented. For each disaster recovery practice, a grand mean was determined and matched with a mean of the firm's business continuation plan. A Pearson correlation was adopted to assess the strength that existed between variables.

The regression equation assumed the following form

$$Y = \beta o + \beta_1 X_1 + \beta X_2 + \beta_3 X_3 + \beta_4 X_4 + \acute{\varepsilon}$$

Where Y = Business Continuity

β_i = (i = 0 – 4) = Regression coefficient

X_1 = Risk Assessment

X_2 = Plan of Action Development

X_3 = Choice of Alternative Recovery Sites

X_4 = Selection of Backup Strategy

$\acute{\varepsilon}$ = Unexplained variables not explained by the model

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

The study objective was determining disaster recovery principles and its influence on business continuation at United Nations Office in Nairobi. Presented in this chapter involves analyzed data and interpretation.

4.2 General information

The demographic information considered in the study were the respondents' highest level of education, length of service and designation at United Nations Office in Nairobi.

4.2.1 Response Rate

A total of 25 questionnaires were issued out and only 19 were given back. This denotes a return rate of 76% which is was satisfactory. It conforms to Mugenda and Mugenda (2003) who put-forth that a return rate exceeding 70% was sufficient.

4.2.2 Length of Continuous Service

This represents the period of continuous service that the respondents had worked at the United Nations Office in Nairobi. It is assumed, ceteris paribus, the longer an employer has been working in an organization, the more versed they are to the operations of the organization. The result is represented in Table 4.1.

Table 4.1 Length of Continuous Service

	Frequency	Percent	Cumulative Percent
Less than two years	2	10.5	10.5
2-5 years	7	36.8	47.4
6-10 years	6	31.6	78.9
Over 10 years	4	21.1	100.0
Total	19	100.0	

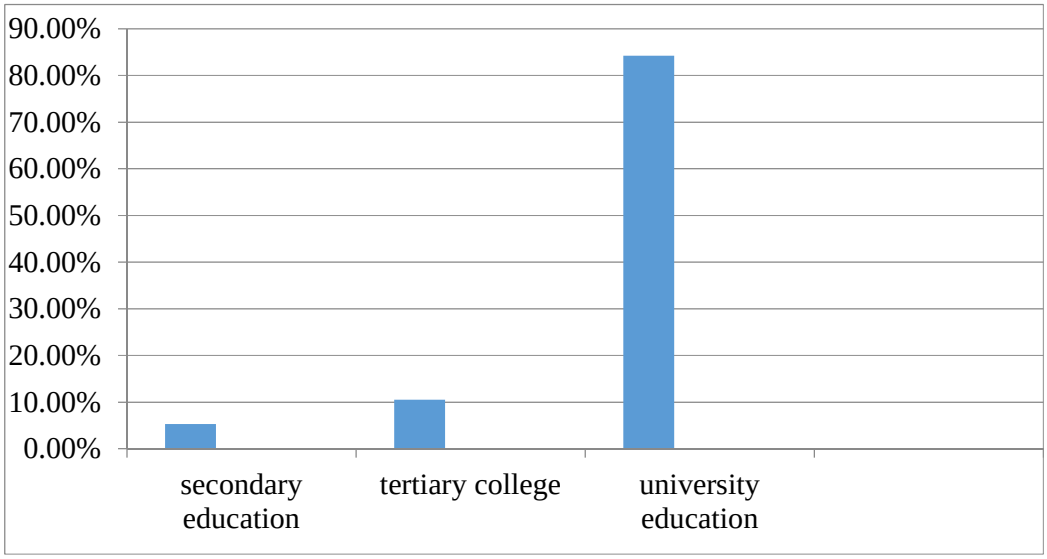
Most respondents had worked between 2-5 years in the organizations while 31.6% of the respondents indicated that they have worked in the United Nations Office for a period of between 6 and 10 years. This means that over two-thirds had worked in the organization between 2-10 years.

This group of the respondents can be considered to be versed with the operations of the organization and will provide valuable information for the research. In addition, 21.1% worked in the institution for over 10 years. Generally, this group of respondnets that were purposely selected were considered to be privy to the role of disaster recovery process and business continuity at UNON.

4.2.3 Level of education

This section sought to find out the academic qualifications of the respondents. The output is depicted in Figure 4.1

Figure 4.1 Level of education



The results on the level of education indicate that majority (84.2%) of the respondents had university degrees while 10% had diplomas and certificates. However, 5.3% of the respondents had secondary level of education but it was found that this cadre of staff had worked for over ten years. This group therefore had more practical job experience and was found to understand equally the research subject matter.

4.2.4 Designation in the Organization

This section sought to establish the respondent's designation at UNON. The output is tabulated below.

Table 4.2: Job Designation

	Frequency	Percent	Cumulative Percent
IT manager	2	10.5	10.5
Business analyst	4	21.1	31.6
Network & System Admin	13	68.4	100.0
Total	19	100.0	

From the findings, most of the respondents (68.4%) were network and system administrators, while 21.1% of the respondents were business analysts. The implication of this findings were that the respondents deal with the day to day ICT functions of the organization and will therefore be an invaluable source to the research data.

4.3 Reliability Test

Reliability was tested to find out if the research instruments utilized gave reliable results. The test of the reliability scales is provided in Table 4.3.

Table 4.3: Output of Reliability Scales

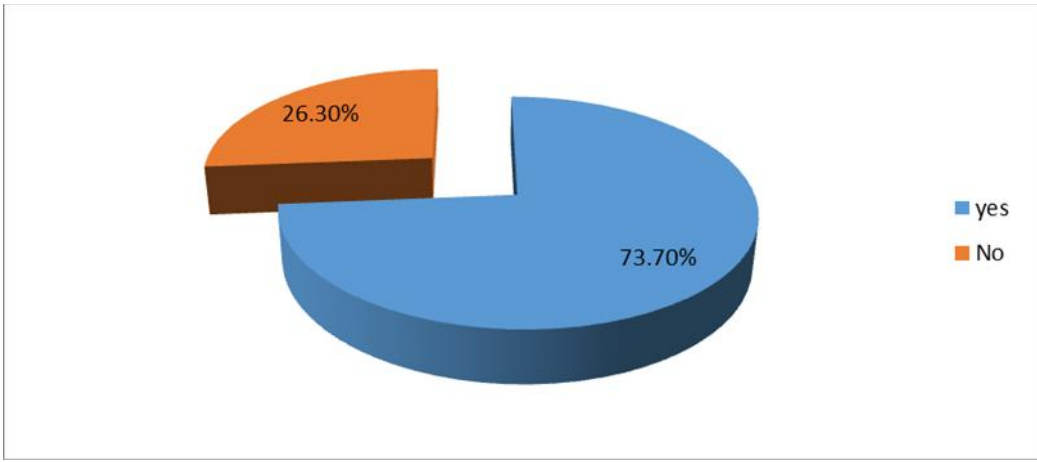
Row	Assessment question	Measure	No. of questions	Reliability
1	6a	Risk Assessment	4	0.873
2	6b	Plan of Action	4	0.782
3	6c	Alternative Recovery site	5	0.821
4	6d	Back up strategy	2	0.844

The results of internal consistency found that Cronbach's alpha was more than 0.7, meaning that the questions comprised in the variables were reliable implying that results were consistent on similar variables.

4.4 Disaster Recovery Process in the Organization

Disaster recovery process seeks to prevent loss of data and continuation of a firm’s operations. This is achieved through aligning organisational resources and employees strategically to counter disaster and support business continuity. On the question of whether UNON had in place adequate disaster recovery plans, majority (73.7%) of the respondents answered to the affirmative. The outcome is give in Figure 4.2.

Figure 4.2: Disaster Recovery Process in the Organization



This implies that there is a small proportion of the respondents who feel that there isn't adequate disaster recovery plans in the organization and it will therefore be necessary to establish why this is so and consequently remedy the situation.

4.5 Disaster recovery practices in United Nation Office.

This section of the questionnaire sought to find out whether disaster recovery practices are being implemented in the United Nation Office. Developing a DRP is meant to identify fundamental stages that aid the firm to recover from loss of data and restoring data assets and this process is anticipated to mitigate confusion and errors. This can be achieved by having a clear recovery plan and ensuring that the employees are prepared to face a disaster. The disaster recovery practices that were discussed in the research include risk assessment, development of a plan of action, choosing an alternative recovery site and selecting a back-up strategy.

4.5.1 Risk Assessment Process

This step involves identifying the effects from disruptions which have an impact on the firm as well as the approaches of quantifying such effects.

This step will therefore be concerned with setting up a recovery plan on the basis of priority and continuity of operations after a disaster.

Table 4.4: Risk Assessment in United Nation Office

Statement	Mean	Std. Deviation
The main areas of vulnerabilities such as electrical power, physical security, fire detection and suppression or computer virus infection exist in the organization	3.842	1.119
The ICT staff periodically take stock of the organizations inventory with an aim of identifying systems and resources to its business operations	3.526	1.124
Continuous consultation with departmental heads of the critical sections is made to evaluate the state of vulnerabilities at a given time	3.105	1.243
The organization has a blue print of the risk assessment which is continuously updated based on emerging risk	2.895	1.150
Overall Mean	**3.342**	

In the assessment of the organization IT function risk, the results show that the identification of the main areas of vulnerabilities such as electrical power, physical security, fire detection and suppression or computer virus infection in the organization (M=3.8421) was the most dominant risk assessment practice. In addition, the organizations ICT staff periodically take inventory of the organization with an aim of identifying systems and resources to its business operations (M=3.5263) as well as the organization having continuous consultation with departmental heads of the critical sections that are prone to disasters. However, this practice had the highest standard deviation (SD= 1.243) meaning that the respondents had different views as far as taking stock of points of vulnerabilities. The other practice which was moderately practiced during risk assessment was that the organization lacked a proper blue print of the risk assessment that is continuously updated based on emerging risk.

4.5.2 Developing a Plan of Action

Producing an action plan can be beneficial to organization as it allows project managers to monitor their progress through comparison of the actual results against the plan as they take each task step-by-step. An action plan allows the organization to operate in a structured manner towards achievement of the main goal. Furthermore, it provides the organization with appropriate foundations and creates a bond between members since members understand their roles. The result on whether UNON have an action plan is presented in Table 4.5.

Table 4.5 Developing a Plan of Action

Statement	Mean	Std. Deviation
Accessibility of the building or at an alternative site by the employees at all times is guaranteed	3.738	1.195
The concerned staff that deal with DR have circulated their contacts that will facilitate quicker reach	3.579	1.346
Each department in the UN office have tailored recovery plan that provide direction on how to quickly resolve the site issue	3.105	1.243
The disaster recovery team in the organization conducts periodic brainstorming sessions for management and corporate employees	2.737	1.240
Overall Mean	**3.298**	

From the findings, it was pointed out that in the event of a disaster, accessibility of the building or at an alternative site by the employees at all times is guaranteed (M=3.738) as well as ensuring that all the concerned staff that deal with disaster recovery are well known by all the staff and there contacts are circulated and are to be contacted whenever there is a disaster (M=3.5789).

Each department in the UN office have tailored made recovery plan that provide direction on how to quickly resolve the site issue (M=3.1053). However, it was found that there was little brainstorming sessions for the management and corporate employees in the organization to plan for disasters and this will require the organization to address this gap in the disaster risk management.

4.5.3 Choosing Alternative Recovery Site

The respondents were told to choose alternative recovery site to be utilized in the organisation on the basis of costs and benefits. The output is demonstrated in Table 4.6.

Table 4.6 Choosing Alternative Recovery Site

Statement	Mean	Std. Deviation
The organization has vendor maintenance agreements under which the vendors are responsible for the data recovery, repair and replacement	3.105	1.410
There exist a quick shipping contract that binds vendors to deliver hardware replacement within a three to five days	2.737	1.558
A hot site exist and is supported by a recovery plan vendor	2.579	1.502
A cold site exist and is supported by the recovery staff	2.263	1.195
The organization has a self-contained mobile trailer that houses all of the computer equipment	2.211	1.512
Overall Mean	**2.579**	

The finding strongly acknowledge that the organization has vendor maintenance agreements under which vendors were mandated to recover data and maintenance (M=3.105) and in addition they have entered into a quick shipping contract that binds vendors to deliver hardware replacement within a three to five days (M=2.7368) whenever a disaster strikes.

The organization further, in the cause of choosing a recovery site have in place recovery hot site which coincides to a recovery vendor plan. The respondents opposed this statement noting that the firm consisted of a self-contained movable trailer where all computer devices were kept (M=2.211).

4.5.4 Selecting a Backup Strategy

Respondents were told to select a back strategy utilized by the organisation. The output is given in Table 4.7.

Table 4.7 Selecting a Backup Strategy

Statement	Mean	Std. Deviation
The organization has an offsite backup system with data encryption and backed up in a remote site for the offsite backup system	3.526	1.504
The organization has an in-house backup system placed at different locations in the building	3.474	1.577
Overall Mean	**3.500**	

From the finding, the organization has, to a moderate extent, backup system with data encryption backed up in a remote site to generate new data set whenever there is a loss (M=3.526). In addition, UNON had put in place an in-house backup system that is placed at different locations in the building (M=3.474) that cannot be affected at the same time whenever a disaster strikes.

4.5.5 Other Disaster Recovery Plan

Apart from the plans enumerated above, the respondents were also asked to enumerate other disaster recovery practices that are being employed by the organization.

The respondent pointed out that Google drive could be used as a backup because the organization has an agreement with the Google and have been allocated extra space for back up purpose as well as having a manual server backup scheduled to tape drives, cloud backup and hot site. Hence, there is an unlimited opportunity for back up using the Google facilities. The other forms of back up being employed by the organization include a manual hard drive/data backup, power disruption maintenance, flash disk and floppy.

It was also noted that the human resources and disaster recovery planning are the key players in handling the issues of disaster in the organization which is communicated to all staff and the need to assure of the organizations business continuity before occurrence of a disaster. Educating employees about disasters preparation and installation of back up and disaster recovery should form part of the culture of the organization.

4.6 Business Continuity Outcomes

The respondents determined the influence of disaster recovery plans on the firm's capacity to pursue its operations after a disaster. Business Continuity Planning concept deals in designing plans which are meant to ensure business continuity. Each business needs to make the necessary preparations to protect staff and the firm's products to enhance business continuation. The outcome is depicted in Table 4.6.

Table 4.8 Business Continuity Outcomes

Statement	Mean	Std. Deviation
Mitigate the duration, severity, or pervasiveness of disruptions that do occur	4.275	0.954
Ensure the continuous performance of essential functions and operations during an emergency,	3.974	0.830
Achieve the timely and orderly resumption of essential functions and the return to normal operations	3.804	0.827
Minimize loss of life, injury, and property damage	3.662	1.024
Provide an integrated and coordinated continuity framework that takes into consideration other relevant organizational, governmental, and private sector continuity plans and procedures	3.505	0.682
Protect essential facilities, equipment, records, and assets	2.956	1.242
	3.696	

The results on the effect of disaster recovery plans on the UNON business continuity show that it manages the duration, severity, or pervasiveness of disruptions that do occur in the event of a disaster (M=4.275) and this they pointed out ensure the continuous performance of essential functions and operations during an emergency (M=3.974). In addition, it was found that disaster recovery plans enables the firm to mitigate disruptions which might arise from disasters. The results showed that disaster recovery plans attained a minimal effect in cautioning the firm facilities, equipment, records and assets (M=2.956).

4.7 Regression Equation

To establish the relationship between DRP and the organizations business continuity in the study, the researcher found the overall mean of each disaster recovery measure used under section 4.5 and section 4.6 and thereupon regressed. From their overall means of each factor, as Gill and Beger (2012) observes that there could be chances of endogeneity which might be contributed by omission of variables. This might lead to measurement errors. To mitigate endogeneity, variables of TQM practices were implemented. Coefficient of determination was utilized to assess the model fitness. The model summary is presented in the Table 4.6 below

Table 4.9: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.652[a]	.425	.357	.281

It was found that the value of adjusted R squared was 0.357, meaning that there existed a variation of 35.7% on business continuity. This is associated with adoption of disaster recovery mechanisms. This suggests that the regression model implemented for this study was reliable.

Table 4.10: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.971	5	0.3285	49.029	.002[b]
	Residual	0.875	13	0.0067		
	Total	2.846	18			

Analysis of variance was found to be significant since the p-value was less than five percent. Computed p-value had a higher value as compared to critical value of 2.27.

This meant that the independent variables significantly influenced firm's business continuity.

Table 4.11: Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	12.977	5.402		3.349	.001
	Risk Assessment= X_1	2.020	.046	.022	.437	.663
	Development of a plan of action =X_2	1.001	.007	.004	.073	.942
	Choosing alternative recovery site=X_3	.059	.045	.072	1.333	.186
	Back-up strategies=X_4	.253	.105	.150	2.404	.018
	Other undocumented strategies=X_5	0.685	.149	.804	11.319	.000

Note: Dependent variable – Business Continuity; X_1 = Risk Assessment; X_2 =Development of a plan of Action; X_3 = Choosing Alternative Recovery Site; X_4 = Back-up Strategies; X5 = other undocumented strategies from the data in the above table, the regression equation obtained is depicted below:

$Y = 2.977 + 0.253X4 + 0.685X5$

Y= Business Continuity

X_4= Back-up strategies

X_5= other documented strategies

Risk assessment, development of a plan of action and choosing alternative recovery site were debarred from the regression model on account of being insignificant. The p-values surpassed five percent as follows: .663, .942 and186 respectively.

Back-up strategies and other undocumented strategies were significant in explaining the link between information technology disaster recovery and business continuity. Their p-values included .018 and .000 respectively.

4.8 Challenges to Implementation of Disaster Recovery Principles

In this section, the researcher determined the challenges which were experienced by the firm in implementation of disaster recovery plans as well as continuity of organisational plans. The results are presented in Table 4.7.

Table 4.12: Challenges to Disaster Recovery

Statement	Mean	Std. Deviation
Difference in work culture	2.947	1.393
Inadequate funding	2.947	1.471
Conflict of interest among influential stakeholders	2.737	1.408
Lack of clear policy guidelines	2.526	1.504
The organization is unable to limit the severity of disruptions	2.474	1.073
Technological challenges	2.421	1.121
Not all the records are protected	2.363	1.383
Lack of senior management support	2.368	1.257
A lack of clear roles and responsibilities	2.368	1.423
Un able to provide a coordinated continuity framework that is inclusive	2.316	.946
Un able fully recover all the lost data	2.263	1.147
Poor supervisory	2.263	1.046
Lack of training ICT technical team	2.211	1.316
Incorrect assumptions in formulating BCP and DRP	2.212	.917
Resumption of essential ICT services take too long	2.105	1.197

The results shows that the common challenges faced by the organization in implementing disaster recovery programs is the difference in work culture and inadequate funding by the organization towards the task (M=2.947). In addition conflict of interest among influential stakeholders and a lack of clear policy guidelines (M=2.526) in the organization was to a small extent pointed out a challenge.

Further, the respondent noted that not all the records are protected and there is a lack of clear roles and responsibilities to the staff. Consequently, in rare occasion, resumption of essential ICT services takes a bit long whenever a disaster befalls the organization.

4.9 Discussion of the Findings

The results have demonstrated that indeed disaster recovery, if not managed well impacts on the level of business continuity process in a firm. Similarly, a well-managed disaster recovery system will lead to continuity in business operations in case a disaster affects the organization. In general, the research reinforced the views that by an organization putting in place an effective recovery plans, the level of disruption on the organizations operations is minimized. This position supports the earlier views of (Swartz, 2008) that DRP minimizes the effects of disaster through taking counter actions which are aimed at protecting important organisational resources that can guarantee the firm continuity of its operations.

The organization DRP follows a number of steps including performing risk assessment, development of a plan of action, choosing an alternative recovery site and selecting a back-up strategy. The risk assessment plan involves steps aimed at profiling all potential risks that the organization faces and involves all departments at UNON. Therefore as Hiles (2003) pointed out, the identification of risks in an organization should consider both financial and non-financial costs. Through this, the firm can keep accurate records and allocate a satisfactory budget for disaster recovery. This is seen as a critical step especially in the planning phase which involves brainstorming by departmental heads. These findings are in harmony with Chow (2007) insists on the importance of assessing risk is identifying any form of threats that can, affect smooth-flow of the firm's operations causing disruptions.

Further, the study found that different organizations face different disaster and as Nollau (2014) who notes that firms that succeed in disaster recover had well defined plans to counter disasters. An example is the use of DR plan. Organization had established different recovery sites as a data recovery strategy. These include both cold and hot sites, as well as entering into contracts with vendors to deliver hardware components within a stipulated short time period. As Kirschenbaum (2006) opine, the issues that are arising when considering a DRP, he insists that firms concentrate on developing a DRP which is inexpensive unlike replacing loss of data. Business Continuity planning dictates the approaches and techniques that should be implemented by businesses to ensure that normal functions of the firm can run after a disaster (Nollau, 2014). Firms should take protective measures, which can guarantee normal operations of the firm after occurrence of a disaster; this is part of disaster recovery which is expected to assist the firm to continue with its operations. Firms can use offsite back systems for this purpose.

Risk assessment and development of a plan of action were found to be insignificant. These results are consistent to Mathenge (2011) who concluded that risk assessment and business continuity plans were insignificant. Undocumented strategies and back-up strategies were found to be significant. This findings is supported Muoki (2010) who found a significant link between business continuity and back-up strategies.

CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The chapter summarizes key findings for this research. The objectives of this study were to investigate the disaster recovery plans at United Nations Office in Nairobi, the challenges faced in the disaster recovery and the effect of disaster recovery plans on the organizations business continuity.

5.2 Summary of the Findings

The study established that disaster recovery process follows a sequence of activities that include risk assessment, development of an action plan, having an alternative recovery plan and establishing a backup system. The risk assessment process involved identification of vulnerable areas and assets which are prone to different forms of risks and profiling the remedial actions to limit the risk. The organizations ICT staff periodically takes inventory of the organization with an aim of identifying systems and resources to its business operations. This process involved consultation with different groups of stakeholders both internal and outside the organization. Further, accessibility of the building or at an alternative site by the employees at all times is guaranteed and the concerned staff's contacts that deal with DR have been circulated to all departments in the organization. Apart from the internal remedial actions it was also found that the organization had entered into vendor maintenance agreements whereby vendors are in charge of recovering data and setting up an offsite backup system.

The study revealed that for effective disaster recovery plan, an organization should change the culture of the staff to be alive to a possibility of different forms of disasters affecting the organization; this provides the organization with appropriate foundations and creates a bond between members since each member is expected to understand their roles in minimizing disasters. Among the benefits derived from implementing BCP and DR include reduced downtime and improved understanding of the business operations by all the employees and increased value of business. As for challenges when implementing BC and DR plans change of project sponsor was highlighted as a common factor, conflict of interest among influential stakeholders, lack of clear policy guidelines and the organization being unable to limit the severity of disruptions.

Risk Assessment, development of a plan of action and choosing alternative recovery site were found to be positively related to business continuity. Other undocumented strategies and back-up strategies were found to be statistically significant in explaining the link between information technology disaster recovery and business continuity. These findings match the results found from a study by Biswas and Choudhuri (2012) on the significance between disaster recovery plans and business continuity.

5.3 Conclusion

This study examined on disaster recovery principles and its effect on business continuity process in United Nation Office Nairobi. From the research findings, it can be concluded that the organization recognizes the danger on its operations as a result of disasters occurring. Organization has different forms of disaster recovery and business continuity which is part of the planning approaches which is critical in supporting continuous delivery and minimizing interruptions of loss of information.

It was found that most respondents observed the stages in several sections of BC and DR planning. The firm should involve all its stakeholders in key decisions and change process to ensure that all their interests are set as priorities. This can be achieved by welcoming their contributions when the firm is setting up plans to counter disasters. These factors provide a clear base for the firm to manage and deal with possible threats. To deal with disasters, the firm should formulate a plan to safeguard the interest of the firm and ensure continuity of business processes. Planning requires business obligations and managerial skills to understand the various dynamics of managing disasters and appropriate action to take. This implies that the top management should be commitment in devising strategies that enable the firm to manage risks, integrate systems and assess them regularly to ensure that they are functioning well including preparing employees on the actions to take whenever disasters strikes.

Further, regression results found that the model adopted for the study was reliable since analysis of variance was significant. Back-up strategies and other undocumented back-up strategies were found to be statistically insignificant even though development of a plan, risk assessment and choosing an alternative recovery site were insignificant.

5.4 Limitations of the Study

Constraints of time and resources limited the scope of the study and necessitated an investigation of a single organisation. This implies that the results of this study are exclusive to UN and cannot be applied to make generalization of international humanitarian organisations.

This study was limited to a descriptive research design that lays more focus on establishing existing link between variables under investigation.

This design cannot be utilized to establish the cause and effect linkage between IT disaster recovery and continuation of business. This would allow the researcher to understand how IT disaster recovery might impact on a firm in the long-term.

The administered questionnaires in data collection, an interview guide would have enabled the researcher to collate first-hand information that is accurate and factual. This kind of information is based on the respondents experience and interaction with the variables under discussion hence more specific and detailed data can be gathered.

5.5 Recommendation Policy Implications

The study recommends there is need to enhance the organizational disaster recovery which will assist in the reduction of performance risk assessment. Disaster recovery helps the organization in tailored recovery and providing direction for remedy in matters that involve site. The study also recommends that there is need to manage and establish ways that a firm can address the interest of all its stakeholders through setting clear policy guidelines and procedures to mitigate disruptions.

The study further recommends that organization need to improve on vendor maintenance agreements where vendors are in charge of data recovery, repair and replenishment. In addition, there is a need for the management to improve on disaster recovery plan which will assist in reduction of damaged hard disk.

5.6 Suggestion for Further Research

The study centered on disaster recovery principles and its effect on business continuity process in United Nation Office Nairobi. A similar study should therefore be done on other Parastatals in Kenya. This will shed more light on the disaster recovery principles and its effect on business continuity process in other Parastatals.

REFERENCES

Altay, N., & Green, W. G.(2006). OR/MS research in disaster operations management. *European Journal of Operational Research,175*,475–493.

Arminio, T, & Truax, T. (2005). *A team approach to emergency management. Disaster Recovery Journal,* 18(3).

Bajgoric, N. (2006). Information systems for e-business continuance: A systems approach. *Kybernetes, 35,* 632-652.

Birkmann, J. (ed.) (2009) *Measuring Vulnerability to Natural Hazards*. United Nations University Press, Tokyo.

Breverman, A. (2006). The missing link in business continuity. *Disaster Recovery Journal,* 19(4), 54-55.

Cerullo,V., & Cerullo, M.J.(2004). Business continuity planning: A comprehensive approach. *Information Systems Management,21*,70–78.

Croy, M. (2004). The business value of data. *Disaster Recovery Journal* 17(3)

Dahlhamer J, & Tierney K. (2010). *Winners and losers: predicting business disaster recovery outcomes following the Northridge earthquake*. Newark, DE: DRC, University of Delaware.

Danes S, Lee J, & Amarpurkar S (2009). *Determinants of family business resilience after a natural disaster*. St. Paul, MN: University of Minnesota.

Drabek, R. (2004). Business continuity: Preparation over prevention. *Accountancy Ireland, 38,* 51-53.

Edrissi,A.,Poorzahedy,H.,Nassiri,H.,&Nourinejad,M.(2013).Amulti-agen optimization formulation of earthquake disaster prevention and management. *European Journal of Operational Research, 229*,261–275.

Farajun, E. (2009). The key to information lifecycle management is cost-effective backup. *Disaster Recovery Journal, 18(4).*

Galindo, G., & Batta, R. (2013). Review of recent developments in OR/MS research in disaster operations management, *European Journal of Operational Research, 230*, 201–211.

Glenn, J. (2010). Business continuity vs. protecting data, *Disaster Recovery Journal*, 19(4), 34-36.

Hiles, A. (2003). *Business Continuity: Best Practices-World Class Business Continuity Management.* Rothstein Associates, Inc.

Hiles, A.(2010). *The definitive handbook of business continuity management*. Wiley.

Jackson, R. (2012). Business continuity: Preparation over prevention. *Accountancy Ireland, 38,* 51-53.

Loscocco K.A & Robinson J. (2001), Barriers to small business success among women. Gender and Society; 5(4):511–32.

Losada, C., Scaparra, M.P, & O'Hanley, J. R.(2012).Optimizing system resilience: A facility protection model with recovery time. *European Journal of Operational Research, 217*, 519–530.

Mathenge, P (2011), Disaster recovery and business continuity plans in Class-A Parastatals in Kenya., *Unpublished MBA project*, University of Nairobi.

Mead D, Liedholm C. (2008). *The dynamics of micro and small enterprises in developing countries,* World Development, 26. East Lansing: Michigan State University.

Muoki, K (2010), *Business continuity planning for a global business operator in less developed economies, a case study of General Motors East Africa*, Unpublished MBA project, University of Nairobi.

Nollau, M.J. (2004). Business continuity planning: A comprehensive approach. *Information Systems Management, 21,* 70–78.

Nyambura, W. (2005), *A Survey of ICT aspects of disaster recovery among companies quoted at the NSE,* Unpublished MBA project, University of Nairobi.

Okolita, K. (2009). *Building an Enterprise-Wide Business Continuity Program* Retrieved from CSO Security and Risk website: http://www.csoonline.com/article/509539/how-to-perform-a-disaster-recovery-business-impact-analysis

Olshansky, R., & Chang, S. (2009). Planning for disaster recovery: Emerging research needs and challenges, *Progressing Planning*, *72*,200–209.

Pitt, M., & Goyal, S. (2013). Business continuity planning as a facilities management tool. *Facilities, 22,* 87-99.

Rastegar, N., & Khorram, E. (2014). A combined secularizing method for multi objective programming problems, *European Journal of Operational Research*, *236*, 229–237.

Slater, D. Hager. (2010). *How to Perform a Disaster Recovery Business Impact Analysis.* Retrieved from http://www.csoonline.com/article/509539/how-to-perform-a-disaster-recovery-business-impact-analysis

Swartz, J. (2003).The route map to business continuity management: Meeting the requirements of BS 25999 BSI.

Turner R, Nigg, J., Heller Paz, D. (2006). Waiting for disaster: earthquake watch in California. Berkeley, CA: University of California Press;

Wallace, M., L. Webber. (2012). *The disaster recovery handbook*. New York: American Management Association.

Webb Gary R, Dahlhamer James M, Tierney Kathleen J (2009). *Predicting long-term business recovery from disaster:* a comparison of the Loma Prieta earthquake and Hurricane Andrew. Newark, DE: DRC, University of Delaware.

Williamson, M., L. Webber. (2002). *The disaster recovery handbook.* New York: American Management Association

Zobel, C. W., & Khansa, L.(2014).Characterizing multi-event disaster resilience. *Computers & Operations Research, 42, 83*–94.

APPENDIX: QUESTIONAIRE

This questionnaire has been designed to assist the researcher collect data concerning Disaster Recovery Principles and its effect on Business Continuity Process at United Nations Office in Nairobi. You have been identified as one of the respondents in this study. The information collected will be used for academic, policy and research purposes only and confidentiality is highly assured.

PART A: GENERAL INFORMATION

1) Which department are you currently working at

……

2) For how long have you been working in the organizations?

a) Less than two years [ ] c) 6-10 years [ ]

b) 2-5 years [ ] d) Over 10 years [ ]

3) What is your highest level of education qualification? (Tick as applicable)

a) Primary Education [ ] b) Secondary education [ ]

c) Tertiary College [ ] d) University education [ ]

4) What is your designation in the organization?

a) IT Manager [ ] b) Business Analyst [ ]

c) Network & Sys Admin [ ]

d) Others (please specify…….

PART B: Disaster Recovery Process in the Organization

5) Does your organization have in place a disaster recovery Plan?

a) Yes [ ] b) No [ ]

6) Please indicate the extent to which the following disaster recovery practices are being applied in the organization. Where **1 - Strongly disagree; 2 -Disagree; 3 - Moderate extent; 4 - Agree; 5 - Strongly Agree**

	DR practices					
	Performing Risk Assessment	**1**	**2**	**3**	**4**	**5**
1	The ICT staff periodically take the inventory of the organization with an aim of identifying systems and resources to its business operations					
2	Continuous consultation with departmental heads of the critical sections is made to evaluate the state of vulnerabilities at a given time					
3	The organization has a blue print of the risk assessment which is continuously updated based on emerging risk					
4	The main areas of vulnerabilities such as electrical power, physical security, fire detection and suppression or computer virus infection exist in the organization					
	Developing a Plan of Action					
1	The disaster recovery team in the organization conducts periodic brainstorming sessions for management and corporate employees					
2	Each department in the UN office have tailored recovery plan that provide direction on how quickly to resolve the site issue					
3	The concerned staff that deal with DR have circulated their contacts that will facilitate quicker reach					
4	Accessibility of the building or at an alternative site by the employees at all times is guaranteed					
	Choosing Alternative Recovery Site					
1	The organization has vendor maintenance agreements under which the vendors are responsible for the data recovery, repair and replacement					

2	There exist a quick shipping contract that binds vendors to deliver hardware replacement within a three to five days					
3	A hot site exist and is supported by a recovery plan vendor					
4	A cold site exist and is supported by the recovery staff					
5	The organization has a self-contained mobile trailer that houses all of the computer equipment					
	Selecting a Backup Strategy					
1	The organization has an in-house back up system placed at different locations in the building					
2	The organization has an offsite backup system with data encryption and backed up in a remote site for the offsite backup system					

7) What other disaster recovery plans does the organization have and employ? Please explain

……

……

……...

Where **1 – Not at all; 2 – Small extent; 3 – Moderate extent; 4 – Large extent 5 – Very large extent**

	Statement					
1	Un able fully recover all the lost data					
2	Resumption of essential ICT services take too long					
3	The Organization is unable to limit the severity of disruptions					
4	Not all the records are protected					
5	Un able to provide a coordinated continuity framework that is inclusive					
6	Difference in work culture					
7	Conflict of interest among influential stakeholders					
8	Lack of senior management support					
9	A lack of clear roles and responsibilities					
10	Inadequate funding					
11	Lack of trained ICT technical team					
12	Lack of Clear Policy guidelines					
13	Technological challenges					
14	Incorrect assumptions in formulating BCP and DRP					
15	Poor supervisory					

Disaster Recovery

On average after systems downtime how many hard drives are damaged beyond recovery

Business Continuity

Questions
Hrs.

(1) On average how many disruptions are experienced per day [ ]
(2) ` How long does it take for the system to resume fully [ ]
(3) On Average how many complaints do you receive [ ]
From users after recovery process
(4) On average what is the extent of physical hard drive damage [ ]

8) The following are some of the Business Continuity outcomes that the organization derives as a result of having disaster recovery plans. Please indicate the extent to which the organization has derived the following benefits from the process.

Where **1 – Not at all; 2 – Small extent; 3 – Moderate extent; 4 – Large extent 5 – Very large extent**

	Statement					
1	Minimize loss of life, injury, and property damage					
2	Mitigate the duration, severity, or pervasiveness of disruptions that do occur					
3	Achieve the timely and orderly resumption of essential functions and the return to normal operations					
4	Protect essential facilities, equipment, records, and assets					
5	Ensure the continuous performance of essential functions and operations during an emergency,					
6	Provide an integrated and coordinated continuity framework that takes into consideration other relevant organizational, governmental, and private sector continuity plans and procedures					

9) What other benefits is realized from the disaster recovery plans put in place, other than those covered above? Please

explain……

……

THANK YOU FOR YOUR TIME.