ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

The Preparedness of Smes for Disaster Recovery and Business Continuity Planning

Olabode Olatubosun
Business Information System
University of Botswana
P.B 007, Gaborone, Botswana, Nigeria
Olabode_olatubosun@yahoo.co.uk

Abstract: Information and infrastructures are vulnerable to risk such as incidences and disasters. To mitigate against these emergencies, disaster recovery plan and contingency plan becomes very essential. This paper present a report of the survey carried out on some small and medium scale Entrepreneurs in Botswana to determine the awareness and preparedness of disaster recovery and business continuity planning. 85 structured questionnaires were administered to personnel of SMEs. It explores the key factors of user awareness, impact as well as the importance of disaster and continuity planning through a research survey thereby gathering empirical evidences. Data collected from 85 respondents was analysed and tested using the frequency distribution. Spearman's Chi Square and Correlation were used to test the variability of the responses, while Crobach's Alpha was used for the reliability test. The results revealed that SMEs know much about disaster recovery and Continuity planning. They are also aware of the type of disaster, its impact, importance of disaster recovery and continuity planning vis as vis the extent to which disaster can affect business activities if disaster recovery and business continuity planning are not adequately put in place.

Keywords: Disaster, Disaster Recovery, Continuity Planning, Information Technology, Attack, Risk, Entrepreneurs

I. INTRODUCTION

Information Technology (IT) and automated Information Systems (IS) are vital elements in most business processes, because these resources are so essential to an organization's success. It is critical that the services provided by these systems are able to operate effectively without excessive interruption (Wings 2000). Turban, McLean, and Wetherbe (1996) describe IT as a system represented by a collection of components such as hardware, software, databases, networks, procedures, objectives, and people operating within the context of a set of cultural norms and values for example, the managerial skills, corporate culture, and organizational structure. Joe and Christoph (2010) note, Information System as a combination of hardware, software and Telecommunications networks that people build and use to collect , create and use to distribute useful data, typically in organization settings. Also in James and Marakas (2009) IS can be any organized combination of people, hardware, software, communications networks, data resources, policies and procedure that store, retrieves, transforms and disseminates information in an organization.

Disaster is an unanticipated incident or event, including natural catastrophes, technological accidents, or human-caused events, causing widespread disruption, loss, or distress to an organization that may result in significant property damage, multiple injuries, or deaths (Goh Moh Heng (1996); ASI (2005). According to Vasant and Ashok (2007) a threats or hazards which measures the probability of an attack on the information assets come in three basic categories. Clearly, natural hazards are ones that can sometimes be anticipated and the effects mitigated; other times, they come without warning and must be responded to. Human-caused hazards also can sometimes be anticipated and other times come as a surprise.

Arnell (1990) note that disaster can cause a significant disruptions in the information services capabilities for a period of time and can affect the operation of the organization. Disasters, though unpredictable by nature, can strike anywhere at any time with little or no warning.

Recovering from one can be stressful, expensive and time consuming, particularly for those who have not taken time to think ahead and prepare for such possibilities (Jeffrey 2009). However, when disaster strikes, those who have prepare and made recovery plans tend to survive with comparatively minimal loss and/or disruption of productivity. A Disaster according to Vasant and Ashok (2007) and Ramesh, Jon, and Ted (2007) is an event that causes a significant and perhaps prolonged disruption in system availability. Business continuity planning (BCP) is a methodology used to create and validate a plan for maintaining continuous business operations before, during, and after disasters and disruptive events (Susan 2007). BCP has to do with managing the operational elements that allow a business to function normally in order to generate revenues. It is often a concept that is used in evaluating various technology strategies.

This article presents a study that investigated the preparedness of the small and medium scale entrepreneurs for recovering their information systems after a disruption and their ability to resume its services within a reasonable time during and after disaster. The study investigated whether local SMEs are aware of disaster recovery and business continuity planning, have knowledge of what kind of disasters that often affect their information systems; seeks to know the magnitude of the distraction or disruption caused by the disasters, how SMEs plan their information systems recovery; determining what kind of preventative measures are used to combat data and assets loss; and to discover the impact of the costs incurred from rebuilding the information systems to resume business.

II. BACKGROUND STUDY

Information systems are faced with risks such as unauthorized modification of programs of data, theft of information, unauthorized access to data, unauthorized use of information assets and compromise of confidentiality of information (Christoph, 2010). Information Systems are exposed to forces of nature, accidental human error or malicious intent of people. If disaster recovery and continuity plan is not put in place, a compromise of these risks could lead to Information System unavailability and business discontinuity, (Vasant and Ashok, 2007)

In a study of companies that experienced a major data loss without having a solid BC/DR plan in place, 43% never reopened, 51% closed within two years, and only 6% survived long-term (Dwyer et al. 1994). Consequently, Savage (2002) observed that after the September 11 attack, most businesses that were directly affected somehow managed to keep alive, some are working at full strength which raises an awareness of disaster recovery or business continuity planning though as far as the agenda should be.

He said that everyone knows that Business Continuity Planning (BCP) is important unfortunately companies never know when it is urgent.

III. RESEARCH MODEL AND HYPOTHESIS

These days, almost all SMEs employed the use of IS in the management of their businesses and as a result, the need to plan for potential disruptions of technology services has increased exponentially. Many organizations and companies are not adequately prepared for systems disasters. Recent research shows that major barriers to preparation include lack of executive support and funding. Adequate funding for disaster recovery efforts requires a shift in priorities of an organization's IT initiatives. In the past, organizations implemented technology as a cost savings measure. Now, IT initiatives that support business continuity and revenue generation are getting top priority (Williamson 2005).

Temporary or prolong disruption to Information Technology Systems may be caused by incidence or disaster and this may lead to degradation of services or even permanent loss of business if the duration and extent of the disruptions are extensive. A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. This vulnerability is a weakness that can be accidentally triggered or intentionally exploited. The threat-source does not present a risk when there is no vulnerability that can be exercised, but in determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities and existing controls. The common threat sources as described in Gary et. al (2002), Ali and Pam, (2009) and Frank (2000) can be Natural Threats (Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events), Human Threats (Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information), Environmental Threats (Long-term power failure, pollution, chemicals, liquid leakage). In the present review, we hypothesize as follows:

H1: Local small and medium scale Entrepreneurs are generally aware of the various type of disaster that can greatly affect their business continuity

Information systems are vital elements in most business processes. Because information system resources are so essential to an organization's success, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. BC planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered quickly and effectively following a service disruption. BC planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the impact level (Marianne, et al 2009).

IT BC planning represents (Marrianne et. al 2009) a broad scope of activities designed to sustain and recover critical IT services following an emergency. IT BC planning fits into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and the facility. Because there is an inherent relationship between an IT system and the business process it supports, there should be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts. In the present review, we hypothesize as follows:

H2: Local small and medium scale Entrepreneurs knows the basic concept, planning and implementation of disaster recovery planning and business continuity

H3: The Local small and medium scale Entrepreneurs have deployed some kind of DRP and BCP measures to prevent lose of information asset and business discontinuity

To avert potential contingencies and disasters or minimize the damage they cause, organizations can take steps early to control the event. BC planning activity is closely related to incident handling, which primarily addresses malicious technical threats such as hackers and viruses. BC planning involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organization's critical functions operating in the event of disruptions to both large and small organization. Daniel et. al (1995) notes, it is impossible to think of all the things that can go wrong, however it is essential to itemize a likely range of anticipated contingency. To do this the contingency scenarios should address each of the resources that can be identified to have support for critical missions and business functions of organization, which can include Human Resources, Processing Capability, Computer-Based Services, Data and Applications, Physical Infrastructure and Documents and Papers. In the present review, we hypothesize as follows:

H4: Local small and medium scale Entrepreneurs knows the type of disaster recovery and continuity planning put in place for their information systems

Risk management encompasses a broad range of activities to identify, control, and mitigate risks to an IT system. Its activities from the IT BC planning perspective have two primary functions. First, risk management should identify threats (Natural, Human and Environmental) and vulnerabilities so that appropriate controls can be put into place to either prevent incidents from happening or to limit the effects of an incident. Second, it should identify residual risks for which BC plans must be put into place.

Information system components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middleware, and applications. Network components can include, such devices as firewalls, sensors (local or remote), switches, guards, routers, gateways, wireless access points, and network appliances etc. Servers include, for example, database servers, authentication servers, electronic mail and Web servers, proxy servers, domain name servers, and network time servers etc. Information system components are either purchased commercially off-the-shelf or are custom-developed and can be deployed in land-based, sea-based, airborne, and/or space-based information systems (NIST Special Publication 2009).

In Marianne et. al (2002) the IT platforms for the Desktop computers and portable systems, Servers, Web sites, Local area networks, Wide area networks, Distributed systems and the Mainframe systems were addressed. For each IT platform type, technical measures were considered from two perspectives. First, the document discusses technical requirements or factors that the BC Planning Coordinator should consider when planning a system recovery strategy and in addition to the information presented on Servers, several factors should be considered when determining the Web site recovery strategy. In the present review, we hypothesize as follows:

H5: The impact of the occurrences of disaster is usually high on information assets of Local small and medium scale Entrepreneurs

H6: Local small and medium scale Entrepreneurs incur minimal looses in the event of disaster because of the adequate provision of disaster recovery and continuity plan

IV. METHODOLOGY

A. *Procedure and Sample:*

A well structured questionnaire was developed based on some specific question that is relevant to estimate the level of the awareness of the Disaster Recovery and Continuity plan in an organization. The research subject were accessible staff of some organizations operating in Gaborone, Botswana. In all 85 staffs of identified organizations participated in the survey. This includes 47 male and 38 female. The personnel across different private sectors (It based and Non IT bases) were randomly selected and where given the questionnaire to record their responses. The questionnaire consisted of two parts. In part one, questions were asked relating to some demographic factors such as gender, Industry type (IT and Non IT based, Year of company existence, Reliance on the use of IS and Involvement of Decision maker in the organizations. Part II consisted of questions relating to Knowledge of DR and BC, Importance of DR and BC, types of Disaster that affect data and assets, Impact of Disaster on IS, Types of DR and BC the organizations have, Kinds of Preventive measures and Efficiency of Preventive measures. The respondents' responses were measured on a four-point likert scale (1-Completely disagree; 2-Agree; 3-Disagree; 4-completely agree). Data was collected from August 2010 to May 2011.

Table 1 Profile analysis of the Respondents

Characteristics	Items	Freq	%
Gender	male female	47 38	55.3 44.7
Industrial Type	IT Based Non IT Based	15 70	17.6 82.4
Year of Existence	1-5years 6-10years > 11years	26 12 47	30.6 14.1 55.3
Reliance on Computer Usage	0-25% 26-50% 51-75% 76-100%	4 10 24 47	4.7 11.8 28.2 55.3
Involve of Decision maker	Yes No	69 16	81.2 18.8

Table 1 depicts the demographic characteristics of the 85 respondents. About 55.3% of the respondents were males while the rest were female. The subject organizations were 17.6% IT based while others were non IT based organizations. The years of existence of the organization were in the distribution of 30.6%, 14.1% and 55.3% for 1-5years, 6-10years and more than 11years of existence. Out of the respondents, 55.3% of them have absolute reliance on the use of IS while other have lower reliance on the use of IS. A high percentage of 81.2% of the respondents feels that the decision makers are involved in the critical decision making of the organizations.

B. *Data Analysis:*

In Table 2, the reliability analysis for the various items of the questionnaire using the cronbach's Alpha is presented. For comparing items in a construct, alpha values greater than or equal to 0.7 is regarded as satisfactory. As in the table, most of the items were reliable as they are greater than 0.7.

Table 2: Reliability Test Analysis

Items	n	Cronbach's Alpha	Number of Items
Knowledge of DR and BC	85	0.719	6
Importance of DR and BC	85	0.758	5
Kinds of Disaster that affect data and assets	85	0.811	9
Impact of Disaster on IS	85	0.423	6
Types of DR and BC the organizations have	85	0.783	7
Kinds of Preventive measures	85	0.564	4
Efficiency of Preventive measures	85	0.786	3

Table 3: Spearman's Correlations for n=85

	1	2	3	4	5	6	7	8	9	10	11
1	1										
2	-.204 .061	1									
3	-.169 .122	.163 .137	1								
4	.138 .207	-.354** .001	-.125 .255	1							
5	-.070 .526	.223* .040	.002 .989	-.400** .000	1						
6	.119 .276	.071 .516	.066 .546	-.256* .018	.154 .159	1					
7	.187 .087	.135 .220	-.121 .271	-.101 .359	-.144 .190	.153 .162	1				
8	-.219* .044	.047 .669	.197 .071	.107 .331	-.142 .196	.210 .054	.185 .091	1			
9	-.006 .957	.247* .023	.104 .343	-.224* .039	.486** .000	.450** .000	-.151 .168	-.075 .497	1		
10	-.202 .064	.106 .335	-.192 .078	-.318** .003	.215* .048	.238* .029	-.077 .483	.004 .968	.405** .000	1	
11	-.122 .265	.214* .049	.039 .721	-.439** .000	.205 .060	.468** .000	.182 .095	.277* .010	.148 .178	.299** .005	1

*. Correlation is significant at the 0.05 level (2-tailed).
**. Correlation is significant at the 0.01 level (2-tailed).

Key: 1-Gender; 2-Type of Industry; 3-Company existence; 5-reliance on Computer; 6-Decision makers; 7-Awareness; 8-Importance; 9-Impact; 10-Type of Disaster; 11-Measure against.

Table 3 presents a summary of the Spearman correlations and their significance indicating the strength of relationship among the decision variables. Out of the 55 pair-wise spearman's correlations 18 pairs of decision variables are significantly correlated. As can be seen from Table 3, Reliance on the use of IS is negatively correlated with the Involvement of Policy maker, awareness of staff on the use of DR and BC, the type of DR and BC employed in the management of IS in organization, the kind of preventive measures deployed and the effectiveness of the preventive measure employed. The Involvement of Policy maker is positively correlated with the type of DR and BC employed in the management of IS in organization and the kind of preventive measures deployed. The awareness of staff on the use of DR and BC is also positively correlated with the type of DR and BC employed in the management of IS in organization, the kind of preventive measures deployed and the effectiveness of the preventive measure employed.

The effectiveness of the preventive measure is correlated with the Impact of Disaster that affect IS and the kind of preventive measures deployed.

Table 4 presents the statistical frequency distribution to determine to what extent does the small and medium scale Entrepreneurs in Gaborone knows about disaster recovery and Contingency planning. The analysis show that 30.6% strongly agree and 69.4% agree that the organization information system has emergency plans that are used in case they incur a disruption that can cause damage or loss to its assets. 35.3% strongly agree, 56.5 agreed while just 10.6% disagree that the disaster recovery and business continuity planning are solidly made for the company's information system. Moreover, the table shows that it is the duty of the information technology department of their organization to make these plans work when need arise with 34.1% and 55.3% of the respondent agreeing while 10.6% of the respondents disagree to this submission. Usually according to the analysis, this emergency plans are formal, well planned for, implemented and executable with high percentages of the respondents agreeing to this and that the organization emergency plans include disaster recovery and Continuity plans for their organization Information Systems. Virtually all the respondents agreed that they understood the essence of having disaster recovery and continuity plans for IS. From Tables 4, out of the 6 posted question on awareness, only the question on "I understand the essence of having disaster recovery and continuity plans for IS" has its frequency not significant with $\chi^2 = 0.012$ and p>0.05.

Others have significant differences in frequency of responses. The result shows, organizations are generally aware of the DR and BC plans for IS of their organizations.

Table 4 Statistical frequency distribution on extent to which the small and medium scale Entrepreneurs in Gaborone knows about disaster recovery and continuity planning.

To what extent does your organization know about disaster recovery and continuity planning?		SA	A	D	SD	χ^2	df	Sig
1	Our organizations information system has emergency plans that are used in case we incur a disruption that can cause damage or loss to its assets.	26 (30.6)	59 (69.4)			12.812	1	0.00
2	These plans are solidly made for the company's information system.	30 (35.3)	48 (56.5)	7 (10.6)		29.812	2	0.00
3	It is the duty of the information technology department of the our organization to make these plans work when need arise.	29 (34.1)	47 (55.3)	9 (10.6)		25.506	2	0.00

4	The emergency plans are formal, well planned for, implemented and executable.	26 (30.6)	46 (54.1)	5 (5.9)	8 (9.4)	50.576	3	0.00
5	The organizations emergency plans include disaster recovery and continuity plans for our Information Systems	38 (44.7)	43 (50.6)	4 (4.7)		31.788	2	0.00
6	I understand the essence of having disaster recovery and continuity plans for IS.	42 (49.4)	43 (50.6)			0.012	1	0.914

Table 5. Statistical frequency distribution on how important is the Disaster Recovery and Business Continuity plans.

How important are the disaster recovery and Contingency plans?		SA	Agree	D	SD	χ^2	d.f	Sig
1	It is important for our organization to have disaster recovery and Continuity plans.	65 (76.5)	16 (18.8)	4 (4.7)		73.718	2	0.00
2	Recovery and continuity plans limits the impact of assets loss during a disaster.	36 (42.4)	35 (41.2)	8 (9.4)	6 (7.1)	38.341	3	0.00
3	Continuity plans reduce the chances of loosing customer loyalty during a disruption.	36 (42.4)	47 (55.3)	2 (2.4)		38.847	2	0.00
4	Effective disaster recovery and business Continuity plans will enable the business to run before, during and after a disaster occurrence.	31 (36.5)	44 (51.8)	10 (11.8)		20.776	2	0.00
5	These plans reduce the risk of losing essential company data and information assets.	53 (62.4)	28 (32.9)	2 (2.4)	2 (2.4)	84.459	3	0.00

Table 5 presents the analysis of the responses using the statistical frequency distribution and show that almost the entire respondent, that is 95.3% agreed except 4.7 that disagree that it is important for a organization to have disaster recovery and Continuity plans. 42.4% strongly agree, 41.2 agree while 16.5% disagree that Recovery and Continuity plans limits the impact of assets loss during a disaster. Continuity plans reduce the chances of loosing customer loyalty during a disruption were the opinion of majority of the respondents but only 2.4% were opposed to this. On whether, an effective disaster recovery and business Continuity plans will enable the business to run before, during and after a disaster occurrence, 36.5% strongly agree, 51.8 agree while 11.8% disagree to this notion of others. It was generally agreed by 95.2% of the respondents that the disaster recovery and Continuity plan will reduce the risk of losing essential company data and information assets.

From Tables 5, the χ^2 value shows that there is significant differences in frequency of responses with $p<0.05$ for all the posted questions on "how important are the disaster recovery and Continuity plans". The result shows the agreement that the disaster recovery and Continuity plans are very important to their organizations.

Table 6 Statistical frequency distribution on whether the effect of natural disasters are more disruptive and occur frequently than human induced or technical disasters based on examples of natural disasters that cause disruptions and loss to information asset.

What kinds of disasters usually affect your Information System?		SA	A	D	SD	χ^2	d.f	Sig
1	Natural disasters are more disruptive and occur frequently than human induced or technical disasters. Examples of natural disasters that cause disruptions and loss to information asset							
	i. Floods	15 (20.0)	36 (29.4)	20 (48.2)	14 (2.4)	14.624	3	0.00
	ii. Earth tremors and earth quakes.	9 (10.6)	32 (37.6)	39 (22.4)	25 (29.4)	13.40	3	0.004
	iii. Storms.	10 (11.8)	55 (64.7)	13 (15.3)	7 (8.2)	72.318	3	0.00
	iv. Power failures.	30 (35.3)	40 (47.1)	11 (12.9)	4 (4.7)	39.094	3	0.00
	v. Land slides	10 (11.8)	19 (22.4)	33 (38.8)	23 (27.1)	12.825	3	0,005
3	Human induced and technical disasters that usually affect our business activities are:							
	i. Viruses	51 (60.0)	27 (31.8)	7 (8.2)		34.259	2	0.00
	ii. Worms and Trojan horses.	35 (41.2)	32 (37.6)	11 (12.9)	7 (8.2)	38.835	3	0.00
	iii. Power failures.	49 (57.6)	32 (37.6)	4 (4.7)		36.447	2	0.00

Table 6 shows the analysis of the statistical frequency distribution on whether the effect of natural disasters are more disruptive and occur frequently than human induced or technical disasters based on examples of natural disasters that cause disruptions and loss to information asset. This question was miss interpreted by respondent because, most of these natural disaster really occur in this part of the country were the survey was conducted. So the opinions from the table were human imagination. However, responses on the Human induced and technical disasters that usually affect business activities, 60% and 31.8% strongly agree and agree respectively that viruses affect business activities while 8.2% disagree. 41.2% and 37.6% strongly agree and agree respectively that worms and Trojan horses also affect business activities while 8.2% disagree. However 57.6% and 37.6% strongly agree and agree respectively that power failure affect business activities while 84.7% disagree.

Table 6 present a χ^2 value and the result show there are significant difference in the frequencies of the posted question with P<0.05. and the result show the level of agreement on the type of disaster that usually affect the IS of an organization.

Table 7 Statistical frequency distribution on to what extent can disasters affecting Information System impact on data and assets of an organization.

To what extent can disasters affecting IS impact on data and assets of your organization?		Strongly agree	Agree	Disagree	Strongly disagree	χ^2	d.f	Sig
1	Disruptions in the daily running of the business can cause a great loss to the company's financial assets, data and information.	50 (58.8)	22 (25.9)	13 (15.3)		26.282	2	0.00
2	Disruptions are frequent in our organization.	2 (2.4)	6 (7.1)	67 (78.8)	10 (11.8)	132.835	3	0.00
3	It can be very costly to resume business after a disruption if there is no emergency plan.	28 (32.9)	40.9 (47.1)	17 (20.0)		9.341	2	0.009
4	It could take about a week or more to resume services after disruption.	16 (18.8)	50 (58.8)	19 (22.4)		25.012	2	0.00
5	We can loss customer value because of our frequent system break downs and service unavailability.	3 (3.5)	11 (11.9)	48 (56.5)	22 (27.1)	54.435	3	0.00
6	We are always able to recover most of our assets after a disaster strike.	15 (17.6)	53 (62.4)	13 (15.3)	4 (4.7)	66.482	3	0.00

Table 7. Shows the statistical distribution on to what extent can disasters affecting Information System impact on data and assets of the small and medium scale Entrepreneurs in Gaborone. 84.7% believed that disruptions in the daily running of the business can cause a great loss to the company's financial assets, data and information while 15.3% are of varying opinion. 78.8% believed that disruptions are not very frequent in their organization, but should in case there is disruption, it can be very costly to resume business after a disruption if there is no emergency plan was the opinion of 80.0% of the respondents while 20.0% disagree with this opinion. 76.6% agree that it could take about a week or more to resume services after disruption while 22.4% disagree. small and medium scale Entrepreneurs in Gaborone can loss customer value because of the frequent system break downs and service unavailability was not acceptable to 83.6% of the respondent because, organizations profits depends on service. They are supposed to provide services to her customers. So citizens at all time must expect service from the small and medium scale Entrepreneurs. However, the small and medium scale Entrepreneurs in Gaborone believed that they can always recover most of their assets after a disaster strike was opined by 80% of the respondents while the remaining 20% object to this opinion. Table 7 present a χ^2 value and the result show there are significant difference in the frequencies of the posted question with P<0.05. and the result show the level of agreement on to what extent can disasters affecting IS impact on data and assets of your organization.

Tables 8 presents the statistical frequency distribution on the kinds of preventative measures that have been deployed by the small and medium scale Entrepreneurs to prevent the occurrence of the disasters. 89.5% agree that the business physical assets are secured in an enclosed fenced area and security team is hired to guard the place. 10.6% did not support the submission. Also, the result shows that 89.4% believed that staffs are trained on proper handling of company assets while 10.6% did not believe. Security coded and passwords are used for accessing the business Information Systems was the opinion of 87% of the respondents while 12.9% disagree with the thought.

Information Systems has a backup performed daily by an appointed Information Technology personnel appointed and copies are secured remotely (off-site) was the believe of 87.1% of the respondents while 12.9% are not of the same reasoning. The value of the χ^2 with p<0.05 suggest a significant difference exist among the responses of the posted question on "what kinds of preventative measures have been deployed by your organization to prevent the occurrence of the disasters". We conclude that organizations are in support of the various adopted techniques applied.

Table 8 Statistical frequency distribution on the kinds of preventative measures that have been deployed by the small and medium scale Entrepreneurs in Gaborone to prevent the occurrence of the disasters

What kinds of preventative measures have been deployed by your organization to prevent the occurrence of the disasters?		Strongly agree	Agree	Disagree	Strongly disagree	χ^2	df	Sig
1	The business physical assets are secured (enclosed in a fenced area and a security team is hired to guard the place)	22 (25.9)	54 (63.5)	9 (10.6)		37.859	2	0.00
2	Staffs are trained on proper handling of company assets.	26 (30.6)	50 (58.8)	9 (10.6)		29.953	2	0.00
3	Security coded and passwords are used for accessing the business Information Systems.	50 (58.8)	24 (28.2)	11 (12.9)		27.835	2	0.00
4	Information Systems has a backup performed daily by an appointed Information Technology personnel appointed and copies are secured remotely (off-site).	39 (45.9)	35 (41.2)	11 (12.9)		16.188	2	0.00

Table 9: How effective are the preventative measures?

	How effective are the preventative measures?	Strongly agree	Agree	Disagree	Strongly	χ^2	df	Sig
1	At any point in time if need be, our recovery and business continuity plans can be very effective.	29 (34.1)	51 (60.00)	5 (5.9)		37.365	2	0.00
2	Our recovery plans and continuity plans are simple and easy to follow.	18 (21.2)	47 (55.3)	20 (23.5)		18.518	2	0.00
3	I can recommend other companies to adopt our plans and change a few items to suit their business needs.	15 (17.6)	49 (57.6)	21 (24.7)		23.247	2	0.00

Tables 9 presents the statistical frequency distribution on how effective are the preventative measures by the small and medium scale Entrepreneurs to prevent the occurrence of the disasters. 34.1% and 60.00% of the respondents strongly agreed and agreed that , at any point in time if need be, their recovery and business continuity plans can be very effective. Only 5.9% disagree with such opinion. On determining how simple and easy to use of the recovery plans and business continuity plans of organizations. 21.2%, 55.3% and 23.5% strongly agree, agree and disagree respectively. Also on the opinion of users of this DR and BC recommending to other companies to adopt their plans and change a few items to suit their business needs. 17.6% strongly agree, 57.6% agree while 24.7% disagree with this opinion. The value of the χ^2 with p<0.05 suggest a significant difference exist among the responses of the posted question on “How effective are the preventative measures”. We conclude that organizations are in support of that the preventive measures are very effective. The frequency analysis as presented in Table 10 suggest the kind of DR and BC their organization have. The χ^2 value with p<0.05 gave the indication that there are significant differences in the frequencies of responses

Table 10. What kinds of recovery and continuity plans does your organization have for their Information systems?

		Strongly agree	Agree	Disagree	Strongly	χ^2	Df	Sig
1	Our company’s Information System has a number of recovery plans	12 (14.1)	65 (76.5)	8 (9.5)		71.459	2	0.00
2	Our systems have remote back up sites	23 (27.1)	55 (64.7)	5 (5.9)	2 (2.4)	83.612	3	0.00
3	We have an emergency team that plans, implements and execute the recovery and contingency plans when need arise.	26 (30.6)	51 (60.0)	8 (9.4)		32.918	2	0.00
4	Our company’s assets are insured to cover for their costs if they get damaged during a disaster strike.	51 (60.0)	29 (34.1)	5 (5.9)		37.365	2	0.00
5	We have remote response services that can be used if the main system has been affected.	22 (25.9)	41 (48.2)	18 (21.2)	4 (4.7)	32.882	3	0.00
6	Our company has a disaster recovery plan that takes into account the business needs, vulnerabilities and risks the business may face.	25 (29.4)	55 (64.7)	5 (5.9)		44.706	2	0.00
7	Our recovery and contingency plans are updated and tested regularly.	23 (27.1)	49 (57.6)	13 (15.3)		24.376	2	0.00

V. CONCLUSION

The analysis suggest that, respondents agreed that small and medium scale Entrepreneurs in Gaborone, know much about disaster recovery and continuity planning. They are also aware of the great importance of disaster recovery and continuity planning vis as vis the extent to which disaster can affect the business activities if the disaster recovery and business continuity planning is not adequately catered for. The types of natural, human or technical disasters/emergency were identified. A careful examination of this analysis reveal that, respondents are biased in their judgment because of the fair of been exposed of their inadequacies, however, for a big organization such as banks establishment, there is the need for a well planned disaster recovery and continuity plan to mitigate against business activities disruption and continuity. Organizations keep large volume of data and need to be preserved.

Organizations need to be prepared for and be able to respond to these attacks. To ensure their survival they must be able to quickly recover their data, continue their operations and protect their reputations. If they do not, losing vital computing resources can bring organization to a standstill and cause them to stop their service delivery function. Effective disaster planning is not optional, but critical for the success of any organizations. To this end, any organization beginning a DRP project should perform a risk assessment for its information technology. This involves checking their network inventory and identifying the resources needed to maintain daily business operations. After analyzing the resources, they must develop a plan of action. This could be a set of procedures or the multiple-volume instruction manual. After developing this plan, the company could integrate it into its business strategies. Also, the company needs to train its employees about specific tasks to be done and how each employee is involved in the process. The implementation process should be reinforced by the company at least once a year by conducting mock disaster scenarios.

A description of Information Systems, Disaster Recovery Planning and Continuity Planning is presented. The survey of the small and medium scale Entrepreneurs in Gaborone gave conclusive results that organization know much about disaster recovery and Continuity planning. They are also aware of the great importance of disaster recovery and continuity planning vis a vis the extent to which disaster can affect the business activities if the disaster recovery and continuity planning is not adequately catered for. Organizations keeps large volume of data and need to be preserved. Disaster are prevalent in recent times in unexpected places around the world, therefore adequate plans need to be put in place for eventuality. Suggested plans and procedure for the design of both plans were reviewed for this purpose. A guide that could assist in selecting, developing and implementing specific technical contingency strategies based on the type of IT system is also presented.

There is a growing reliance upon IT in many organization to the point of mission criticality. IT continuity plan should be applied to install information systems and the new information services whose continuity and reliable functioning may be vital to the organization. IT contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption. Continuity planning generally includes one or more of the approaches to restore disrupted IT services: Restoring IT operations at an alternate location, Recovering IT operations using alternate equipment and Performing some or all of the affected business processes using non-IT (manual).

VI. REFERENCES

[1]. jayi G. O. (2003) e-Government in Nigeria's e-Strategy; The Fifth Annual African Computing & Telecommunications Summit, Abuja, Nigerin.

[2]. Arnell, A (1990), Handbook of Effective Disaster/Recovery Planning, McGraw-Hill Pub. Co., New York, NY, P333.

[3]. Daniel F. Sterne, David M. Balenson, Martha A. Branstad, Lisa M., Jaworski, Theodore M.P. Lee, Charles P. Pfleeger, Sharon P. Osuna, Diann K. Vechery, Kenneth, M. Walker, and Thomas J. Winkler (1995), An Introduction to Computer Security: The NIST Handbook. National Institute of Standards and Technology. Special Publication 800-12.

[4]. Development Workshop entitled “e/m-Government in Africa, Progress Made and Challenges Ahead” in Ethiopia in February 17-19, 2009. Ethiopia. http://www.unpan.org and http://www.uneca.org/aisi/.

[5]. Dwyer, P.D, Friedberg, A.H and McKenzie, K.S. (1994), “It can happen here: the important of continuity planning”, IS Audit & Control Journal, Vol. 1, pp30-35.

[6]. Frank H. Cervone (2006). Managing Digital Libraries: The View from 30,000 Feet. Disaster Recovery and Continuity Planning for Digital Library Systems. Emerald Group Publishing Limited Vol. 22 No. 3, 2006, pp. 173-178. DOI 10.1108/10650750610686234.

[7]. Gabriel O. Ajayi (2003) NITDA and ICT in Nigeria, 2003 Round Table on Developing Countries Access to Scientific Knowledge, The Abdus Salam ICTP, Trieste, Italy. http://www.ejds.org/meeting2003/ictp/papers/Ajayi.pdf.

[8]. Gary Stoneburner, Alice Goguen, and Alexis Feringa (2002). Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology,, NIST Special Publication 800-30.

[9]. Information Technology Research (2002), Vision for IT-Enabled Enhancement of Government Innovation, and E-Government Committee on Computing and Communications Research to Enable Better Use of Information. Technology in Government, National Research Council ISBN: 0-309-50031-1, 168 pages, 6 x 9, (2002) This PDF is available from the National Academies Press at: http://www.nap.edu/catalog/10355.html.

[10]. James O’Brien and George M. Marakas (2009). Management Information Systems, McGraw-Hill International Edition, Ninth Edition.

[11]. Jeffry P Back (2009). Business Continuity and Disaster Recovery Planning. Cited from the Internet on 18 April, 2010. www.oncoreassociates.com/.../Business_Continuity_and_Disaster_Recovery.pdf.

[12]. Joe Valaciach and Christoph Schneider (2010), Information Systems Today, Pearson, Forth Edition.

[13]. John Williamson (2005). Business Continuity Planning A Primer for Management and IT Personnel. Business Continuity Planning. The Any KeyNow Group

[14]. Kritzinger E. and Smith E. (2008). Information Security Management: An Information Security Retrieval and Awareness model for industry Computer and Security 27: 224-231.

[15]. Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, Ray Thomas, (2002). Contingency Planning Guide for Information Technology Systems. National Institute of Standards and Technology (NIST). Special Publication 800-34. bookstore.gpo.gov.

[16]. NIST Special Publication 800-53,(2009). Recommended Security Controls for Federal Information Systems and Organization).http://permanent.access.gpo.gov/lps117689/800-53-rev3-IPD.pdf.

[17]. Ogechukwu Iloanusi, N. and C. Charles Osuagwu (2009), ICT in Education: Achievements so far in Nigeria, Research, Reflections and Innovations in Integrating ICT in Education, http://www.formatex.org/micte2009/book/1331-1335.pdf.

[18]. Patricial J. Pascual (2003), e-government, e-ASEAN Task Force, UNDP-APDIP, These e-primers are also available online at www.eprimers.org. and www.apdip.net.

[19]. Prepared by The AnyKeyNow Group, www.anykeynow.com.

[20]. Price, Robin (1983). Preparing for disaster. Journal of the Society of Archivists, Apr83, Vol. 7 Issue 3, p24, 6p.

[21]. Ramesh R. Rao, Jon Eisenberg, and Ted Schmitt (2007) Improving Disaster Management: The Role of IT in Mitigation, Preparedness, Response, and Recovery. National

Academies Press, downloaded from: http://www.nap.edu/catalog/11824.html.

[22]. Semer, L.J (1998), "Disaster recovery planning for the distributed environment", Internal Auditor, Vol. 55 No.6, pp.41-7.

[23]. Smith, M. and Sherwood, J. (1995), “Business Continuity Planning”, Computer & Security, Vol. 14 No. 1, pp 14-23.

[24]. Steve M. Hawkins, David C. Yen and David C. Chou (2000). Disaster recovery planning: a strategy for data security Information Management & Computer Security, 8/5. MCB University Press. http://www.emerald-library.com.

[25]. Susan Snedaker (2007). Business Continuity and Disaster Recovery Planning for IT Professionals. Syngress Publishing, Inc. Elsevier, Inc.

[26]. Timan Goshit (2009), Nigeria’s Need for ICT SP.259 Technology and Policy in Africa. Cited from Internet on 26, May 2010. http://ocw.mit.edu/NR/rdonlyres/Special-Programs/SP-259Spring-2006/891209EE-E63B-4617-BA9D-7635A63C754B/0/goshit.pdf.

[27]. Turban, E., McLean, E., and Wetherbe, J. (1996). Information Technology for Management. New York, NY.: Wiley and Sons.

[28]. Vasant Raval and Ashok Fichadia (2007). Risk, Control and Security: Concepts and Application. John Wiley & Son.

[29]. Wing S. Chow and Wai On Ha (2008). Determination of the Critical Success Factor of Disaster Recovery Planning for Information System, Information Management & Computer Security. Vol 17. No 3. PP248-275.

[30]. Wings S. Chow (2000). Success Factors for IS Disaster Recovery Planning in Hong Kong, Information Management and Computer Security. MCB University Press, ISSN 0968-5227, 8/2, 80-86.

[31]. Wrobel, L.A. (1997), The Definitive Guide to Business Resumption Planning, Artech House, Norwood, MA.