Assessing the Organizations' Disaster Recovery Preparedness : A Study of SMEs in Zimbabwe

[1]Khanyisa Malufu

[1]Department of Computer and Management Information Systems
Solusi University, Bulawayo, +263, Zimbabwe

Abstract - Information Systems remain a subject to attack by natural and human threats. Security breaches and damages of information systems are increasing daily yet there are still chances of natural disasters affecting availability of Information Systems. As a result, automated data are more susceptible to destruction, unavailability or loss. The aim of this study was to assess whether or not the Small and Medium Enterprises (SMEs) are adequately prepared to recover and resume their operations in the event of a disaster occurring. The researcher chose a descriptive-quantitative research design. Data was collected using a self-constructed questionnaire. Convenience sampling and stratified random sampling techniques were used to select the main subjects of the study. Generally there was no significant difference between the perceptions of SMEs management and non-management personnel on the disaster recovery preparedness of SMEs. The study recommends further future studies to explore ways in which SMEs can be helped to appreciate the importance of disaster recovery planning.

Keywords - *Disaster Recovery Plan, System Availability, Information Security, Compliance, Computer Threats*

1. Introduction

Information Systems remain a subject to attack by natural and human threats. Security breaches and damages of information systems (IS) are increasing day by day yet there are still chances of natural disasters affecting availability of Information Systems. As a result, automated data are more susceptible to destruction, unavailability or loss. Besides, there are still other challenges like power failure that can render systems unavailable. Laudon & Laudon, [1] concur that, Security and reliability are absolutely critical in information systems, because errors, fraud, and disruption of service can lead to large monetary losses and the erosion of customer confidence in those companies and even the entire industry. Data and ISs should be available and accessible as and when needed. The continued operations of these organizations depend fully on the management's awareness of potential disasters, their ability to develop a plan to minimize disruptions of critical functions and the capability to recover operations expediently and successfully. [11]

Most of the Small and Medium Enterprises (SMEs) are funded by the government through loans and grants as means of employment creation, economic empowerment of citizens and indigenization of businesses [13]. In its vision, the Ministry of Small and Medium Enterprise Development strives to "be the 'nerve' centre for economic growth and empowerment through the development of SMEs in Zimbabwe" [14]. Currently, the SMEs in Zimbabwe are the major drivers of the economy and they account for about 70 per cent of the economically active Zimbabweans. Thus, the failure of the SMEs may adversely affect the country's economy and in turn, the lives of many people. Use of Information Systems in order to improve the efficiency in the delivery of services is to be welcome as a noble move and a great step towards improving the performance of the SMEs in line with the advancements in technology. Organizations that seek to make a difference should harness the latest technologies and stay abreast with the industry's competition if they are to remain profitable with an edge over their rivals. However, if such technology is not yet fully understood especially by the people who should implement it, monitor its performance, ensure its security and constant availability, then the organization is greatly increasing its chances of failure if it is attacked. This research seeks to find out if SMEs are adequately prepared for continuity in the event of a disaster. The researcher used a self-constructed questionnaire. As far as the researcher knows, no studies had been made before that addresses the disaster preparedness of SMEs in Zimbabwe as a developing country. This gave the researcher a ground breaking experience as the research is original and not a mere reproduction of other people's ideas.

In the order of consideration, the author first examines some insights from the literature and conceptual framework. Following the examination of the literature and the discussion of the conceptual framework, the researcher proposes research questions and related hypotheses that are tested using the Statistical Package for Social Sciences (SPSS).The research methodology is outlined, followed by the analysis of the data, and discussion. Finally, the conclusions are drawn and recommendations for further future research are made

2. Literature Review and Theoretical Framework

This section presents the theoretical framework, developed from literature upon which the concepts or themes of the study were based. The review of related literature cantered mainly on various computer threats and ways of mitigating risks.

2.1 Disaster Recovery

Disasters are never planned but they may occur at any time. Thus, organisations need to be adequately prepared to continue with business in the event of their occurrence. Recovery strategies should be developed for Information systems, applications and data. This includes networks, servers, desktops, laptops, wireless devices, data and connectivity. The recovery time for IS resources should match the recovery time objective for the business function or process that depends on the IS resource [11]. Some business applications cannot tolerate any downtime and therefore have to be mirrored but this is expensive [12]. However, for small to medium sized businesses with critical business applications and data to protect they can utilise low cost internal or vendor supported strategies. Hardware at an alternate facility can be configured to run similar hardware and software applications when needed. Assuming data is backed up off-site or data is mirrored between the two sites, data can be restored at the alternate site and processing can continue [11]. Besides, there are vendors that can provide "hot sites" for IS disaster recovery. These sites are fully configured data centres with commonly used hardware and software products [12]. Subscribers may provide unique equipment or software either at the time of disaster or store it at the hot site ready for use. Data streams, data security services and applications can be hosted and managed by vendors. This information can be accessed at the primary business site or any alternate site using a web browser. If an outage is detected at the client site by the vendor, the vendor automatically holds data until the client's system is restored. These vendors can also provide data filtering and detection of malware threats, which enhance cyber security. [9][12]

2.1.1 Disaster Recovery Planning

According to Alter [15] disaster recovery plan is a plan of action to recover from occurrences that shut down or harm major information systems. It is a comprehensive statement of consistent actions to be taken before, during and after a disaster. The plan should be documented and regularly tested to ensure the continuity of operations and availability of critical resources in the event of a disaster [11]. The primary objective of disaster recovery planning is to protect the organization in the event that all or parts of its operations and /or computer services are rendered unusable. Preparedness is the key. [1] Laudon and Laudon states that, clients of telecommunications providers with computers and switching centres in or nearby the World Trade Center (WTC) lost service and were stalled with busy signals for at least three days when the WTC and the Pentagon were destroyed on the morning of September 11, 2001.

However, Merrill was able to resume its business later in the day. The firm did not suffer as much as others because it had redundant telecommunications capabilities and a rock-solid disaster recovery plan. Whether provided for internally or by a third party, management should plan for recovery of critical systems and develop alternate operating processes for use during service disruptions [7]. It is essential for any business to have a disaster recovery plan "to make sure that regular processing will resume with minimal pain and inconvenience if the computer system goes down" [15]

Testing is what indicates the effectiveness of a plan. Therefore, it is important that as much care be exercised in testing the plan as in developing it [11]. With passage of time, the plan's effectiveness may be eroded due to environmental changes which occur as organizations change. Some of the changes may render a plan incomplete or inadequate. There could be technological, economic, political, legal, social, or personnel changes that may necessitate the revision of the plans [12]. Besides, the organization may experience personnel turnover or even have the employees forgetting the most critical elements of the plan [10]. Therefore, regular testing of the plan is very important to enable the organisation to identify the areas that need improvement, demonstrate the organisation's ability to recover, determine the feasibility and reliability of the process among other things. Several types of testing can be

performed by the organization, including structured walk-through testing, checklist testing, simulation testing, parallel testing, and full interruption testing. Disasters or problems that occur during the normal course of business should also be documented and included in the plan. [11]

2. 2 Commitment of the Management

Laudon and Laudon [1] suggest that management is responsible for developing the control structure and quality standards for the organisation. Key management decisions include establishing standards for systems accuracy and reliability, determining an appropriate level of control for organisational functions and establishing a disaster recovery plan. Many organisations that have realised the importance of the information systems have the director responsible for the information systems department. However, the size of an organisation also determines what positions can be employed. The highly qualified information systems personnel are very expensive to hire and retain, hence most SMEs do not afford them. Some are even run by inexperienced personnel with minimal qualifications. The owners tend to run their own organisations and some employ their family members and friends even when they have inadequate skills in a bid to cut the costs of doing business.

Whatsoever the case may be, it should be noted that the process of developing a disaster recovery plan is very involved. As Wold [11] puts it, it includes obtaining the commitment and support of the top management who should be responsible for coordinating the disaster recovery plan and ensuring its effectiveness within the organization; establishing a planning committee including representatives from all functional areas of the organisation, which will oversee the development and implementation of the plan; perform a risk assessment and business impact analysis that includes a range of possible disasters, including natural, technical and human threats. [3] Furthermore, there is need to identify the most mission-critical applications, the files they use, and where these files and applications are located and to develop an action plan for handling mission critical applications, such as using manual process or running these applications at a disaster recovery service or backup computer system at another location [12]. Management should have sufficient knowledge and commitment for them to successfully drive the development and implementation of the disaster recovery plan. Besides, for the successful implementation of the plan, there is need for meaningful employee involvement in the whole process [4][3].

2.3 Behavioural Expectations

As stated by Laudon and Laudon [1] the behavioural expectations of an organisation are encoded in its policy manuals and signs posted on bulletin boards. However the behaviour that organisation members internalise is also critical to the success of disaster recovery efforts. Furthermore, employees should clearly understand what is expected of them in case of disaster, what is prohibited, and the extent of their rights and responsibilities and even how disaster will be funded [1]. Lomash and Mishra [10] state that, due to competition it has become difficult for many organisations to retain trained and experienced employees. It is in the light of the above fact, that the SMEs might be having less qualified and inexperienced employees who do not understand the disaster recovery plans of their organisations. Other human limitations increasing the risks include complacency and carelessness [5], and limited ability to understand the business operations [4] and let alone, the value of information systems. According to Layton [9] people in the organisation need to be informed of the risks that are possible in the organisation and the control measures put in place and also what is expected of them so that they can do it. If the responsible people in the organisation are aware of the risks and the control measures that have been implemented within their environment, it is reasonable to assume that there will be an environment of heightened awareness with the promise of fewer chances of non-compliance [7][8]. There are a few core requirements common to almost all data compliance regulations. Data needs to be secure, original, and accessible over many years and be made available in short order if requested [9]. Understanding exactly which regulations apply to one's organization may be very complex and involving. This may seem like an insurmountable challenge but it is possible to deploy a foundation for compliance without complete knowledge of regulatory obligations which will support your compliance needs into the future and provide substantial business benefits [8][9].

2.4 Risk Control

Laudon and Laudon [1] suggest that computer crime is the commission of illegal acts through the use of a computer or against computer systems. The systems programmers, operators and administrators can disable protective features, replace the supervisors or reveal protective measures and thus making the system vulnerable to attacks. The maintenance staff can disable hardware devices or use the stand alone utility programs to attack the system [5]. Thus the system is not safe even from the same hands which seek to protect it [7]. With

frequent power surges, blackouts and brown outs in Zimbabwe, systems outage and even damage of the hardware or software are also a major risk. Therefore, Fault-tolerance or graceful degradation that enables a computer based system to continue operating properly in the event of the failure of some of its components is a necessity [1]. To ensure recovery, system backup is pertinent [6]. There is also need for backup power source to enable operations to continue even in case of power outage. Other threats include the viruses that wreak havoc on the networks, hacking, data diddling, and even the physical damage or theft of equipment [5][2].

The researcher derived the following research question from the above literature and theoretical framework for the purposes of this paper:

Research Question: How prepared are SMEs to continue with business in the event of a disaster with respect to meeting the requirements for disaster recovery planning.

3. Research Methodology

Questionnaires were distributed to 40 managers and 80 non managers from 40 SMEs in Zimbabwe. Zimbabwe has a large number of SMEs; however most of them have not yet computerized their operations. The research used a quantitative descriptive method to assess the preparedness of SMEs to recover from disasters in the event of their occurrence. The respondents used for the questionnaires were picked and chosen according to their years of experience and qualification in order to guarantee that they had the necessary computer skills and knowledge of their organizations. Evaluation and scoring of responses on the questionnaires is as shown in Figure 1 below.

Scale	Responses	Verbal interpretation	Mean Interval
1	Strongly Disagree	Hardly ever the practice	1.00– 1.50
2	Disagree	Rarely the practice	1.51– 2.50
3	Undecided	Neutral	2.51-3.50
4	Agree	Usual practice	3.51-4.50
5	Strongly Agree	Regular practice	4.51-5.00

Figure 1: Evaluation and scoring of the questionnaires

Any scores in the range of 4 and above were accepted as representing that the SMEs have adequate plans for disaster recovery as the respondents expressed that they agree, whilst scores in the range of 3 and below were taken to mean that the SMEs are not adequately prepared to recover from disaster in the event that it occurs. The test value of 4.0 was therefore used as it is the minimum of the acceptable range of 4 to 5. Any values deviating from the test value were checked if they were on the upper or lower end. The higher values were showing that respondents strongly agreed that SMEs are adequately prepared to recover from disaster in the event that it occurs.

4. Analysis of Data

The table 1, below shows the demographic characteristics of the respondents in terms of their work experience. The majority of the employees were experienced as the results show that at least 75% of the respondents had worked for the SMEs for more than 4 years and they therefore understood better how their organizations conduct their day to day business. They had observed at least how work is carried out, knew the organizational culture and at least knew the areas that are given greater priority in their organizations. This means that their responses were more accurate and a true representation of what actually takes place in their organizations.

Table 1: Respondents` work experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 - 4 yrs	30	25.0	25.0	25.0
	5 - 9 yrs	47	39.2	39.2	64.2
	10 yrs +	43	35.8	35.8	100.0
	Total	120	100.0	100.0	

The table 2, below shows the demographic characteristics of the respondents in terms of their qualifications in information technology related training.

Table 2: Information Technology related training

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	None	48	40.0	40.0	40.0
	Certificate	30	25.0	25.0	65.0
	Diploma	28	23.3	23.3	88.3
	University Degree	14	11.7	11.7	100.0
	Total	120	100.0	100.0	

According to the results from the table 2 above, at least 60% of the respondents had some qualification and training knowledge in information technology. However, only 11.7% had pursued it to degree level. Their expectations and their judgment when it comes to the security of information systems was therefore considered

to be more reliable as they responded to things they at least have heard of or actually work with in their day to day activities. In general, it can be assumed that the respondents had at least the basic knowledge required for them to respond to the questionnaire which was administered to them.

When it comes to the level of preparedness of the SMEs to recover in the event of an occurrence of a disaster, the results in table 3 below show that a t-test was performed using a test value of 4.0 at 5% level of significance. Any scores in the range of 4 and above were accepted as representing that the organizations were prepared for disaster recovery with respect to those elements whilst any values in the range of 3 and below represented that the organizations were generally not adequately prepared for recovery in case of a disaster occurring. The test value of 4.0 was therefore used as it is the minimum of the acceptable range of 4 to 5.

Table 3: Disaster recovery preparedness (One-Sample T-test)

N = 120 df = 119 Test Value = 4.0

	Mean	Std. Deviation	Std. Error Mean	Sig. (2-tailed)	Mean Difference
Disaster recovery Planning	1.8883	.38177	.03485	.000	-2.11167
Commitment of the Mgnt	2.7150	.38253	.03492	.000	-1.28500
Behavioural Expectations	3.7056	.67527	.06164	.000	-.29444
Risk Control	4.2479	.42319	.03863	.000	.24792
Average Preparedness	3.1392	.24801	.02264	.000	-.86080

Any values deviating from the test value were checked if they were on the upper or lower end. The higher values were showing that respondents strongly agreed that those particular elements of disaster recovery planning were adhered to. From the 4 dimensions that were tested, the following results were obtained:

Average preparedness has a very low mean of 3.1392 and a standard deviation of 0.24801 as shown in table 3 above. These results as show that the preparedness of the SMEs is significantly lower than expected with a mean difference of -86080 which essentially means that SMEs may not be able to resume their business or continue their operations if they were to be affected by a disaster.

Disaster recovery planning has with a mean of 1.8883 testifies that there are no plans put in place by the SMEs to assist them with speedy recovery. Further analysis was sought and the elements that were checked are presented in table 4 below, which shows that all the items are significantly lower than the test value.

Table 4: Disaster recovery planning (One-Sample T-test)

N = 120 df = 119 Test Value = 4.0

	Mean	Std. Deviation	Std. Error Mean	Sig. (2-tailed)	Mean Difference
Updated asset register	1.9917	.76142	.06951	.000	-2.00833
Assessing of potential disasters	2.0500	.84863	.07747	.000	-1.95000
documented Disaster Rec. Plan	1.8917	.79701	.07276	.000	-2.10833
Documenting of problems	1.7417	.76142	.06951	.000	-2.25833
Regular testing of Disaster Rec. Plan	1.7667	.76404	.06975	.000	-2.23333

The results show that, the respondents generally disagree that their organizations keep an updated asset register, assess potential disasters, have a disaster recovery plan and document the problems that they face during their operations. This is a cause for concern as their recovery from disaster is just left to chance.

Commitment of the management is below the expectations, with a mean of 2.7150 which is significantly lower than the test value of 4.0. However, further analysis as presented in table 5 below shows that whilst there is no disaster recovery committee, no involvement of the top management in developing or supporting of the development of the disaster recovery plans and no functional areas being represented as the whole process is non-existent, the SMEs that have computerized their operations have access to reliable and qualified IT personnel who are in charge of their information systems.

Table 5: Commitment of the Management (One-Sample T-test)

N = 120 df = 119 Test Value = 4.0

	Mean	Std. Deviation	Std. Error Mean	Sig. (2-tailed)	Mean Difference
Top management support	1.8750	.77310	.07057	.000	-2.12500
Disaster rec. committee	1.8500	.77405	.07066	.000	-2.15000

presence					
Functional areas representation	1.7167	.55281	.05046	.000	-2.28333
Reliable IT person	4.0833	.94008	.08582	.333	.08333
Qualified IT personnel	4.0500	.89677	.08186	.543	.05000

The results generally show that whilst the disaster recovery plans are not in place, the management is committed to ensure their information systems are handled and controlled by the people who have the knowhow.

Behavioural expectations stood at the mean of 3.7056 which is also like other factors lower than the expected value.

Table 6: Behavioural expectations (One-Sample T-test)

N = 120 df = 119 Test Value = 4.0

	Mean	Std. Deviation	Std. Error Mean	Sig. (2-tailed)	Mean Difference
Awareness of potential risks	3.6417	1.17248	.10703	.001	-.35833
Communic. expect. to employees	3.8583	.87251	.07965	.078	-.14167
New employee orientation	3.6167	1.13895	.10397	.000	-.38333

Table 6 above shows that in general though above the range of 3.0 and closer to 4.0, they were falling short as new employees were not adequately oriented and made aware of what they are expected to do in the event of a disaster occurring, nor were they made aware of the potential disasters.

This is an indication that the organizations were not assessing the potential risks and hence the employees were in general not aware of the potential risks associated with the use of IT and other risks in doing their business. Closer to the expected value is communicated expectations to employees, this shows that employees were made aware by their organizations as to what is expected of them although that was not enough as it remained at lower levels.

Risk control with a mean of 4.2479 as shown in table 3stands significantly higher than the test value. The SMEs are putting in place some risk control measures to ensure they have constant availability of their information systems.

Table 7: Risk control (One-Sample T-test)

N = 120 df = 119 Test Value = 4.0

	Mean	Std. Deviation	Std. Error Mean	Sig. (2-tailed)	Mean Difference
Backup power source	4.2667	.84747	.07736	.001	.26667
Back up of critical systems	4.0083	.78318	.07149	.907	.00833
Security of premises	4.4500	.68415	.06245	.000	.45000
Password protection	4.2667	.68272	.06232	.000	.26667

They have backup power sources in place as shown by the mean of 4.2667 in table 7. This could be because of the massive power cuts and high electricity bills that they have resorted to buying inverters, solar systems and or generators. The results show that they back up their critical systems and information, they have their premises guarded and they protect their computers and critical systems with use of strong passwords.

Research Question: Is there a difference between the perceptions of management and non-management on the SMEs preparedness to recover in the event of a disaster occurring?

There are basically four elements that were measured to determine if the perceptions of management and non-management differ with respect the preparedness of their organizations to recover from any disaster in the event that it occurs. Table 8, below shows the mean scores of management versus mean scores of non-management for each element that was measured.

Table 8: Group statistics for perceptions

	Current Position	N	Mean	Std. Deviation	Std. Error Mean
Disaster recovery Planning	Management	40	1.7500	.38096	.06023
	Non-management	80	1.9575	.36519	.04083
Commitment of the Management	Management	40	2.6700	.36388	.05753
	Non-management	80	2.7375	.39181	.04381
Behavioural Expectations	Management	40	3.7917	.66103	.10452
	Non-management	80	3.6625	.68229	.07628
Risk Control	Management	40	4.1375	.49339	.07801
	Non-management	80	4.3031	.37462	.04188
Average	Management	40	3.0873	.26598	.04205

Preparedness	Non-management	80	3.1652	.23598	.02638

The values were summarized in variable, average preparedness. This average preparedness was used to determine the overall responses of the respondents as to whether or not they perceived that their organizations were adequately prepared or not. Basing on the average preparedness score there is no significant difference between the perceptions of management and perceptions of non-management. However, it is noted that they both perceive their organizations as inadequately prepared to recover in the event of a disaster occurring.

5. Conclusion and Recommendations

This study concluded that to a greater extent, the SMEs are not prepared for recovery in the event of a disaster occurring. Many of the critical issues are left unattended to as they are not known to them. However, some form of backup is done in most of the organizations although its safety is still questionable. Their recovery from disaster will only be a matter of chance, not that the organizations have done anything to ensure that they continue in business.

The study recommends further future studies to explore ways in which the SMEs can be helped to appreciate the importance of disaster recovery planning.

Acknowledgments

First, the author thanks Solusi University's Office of Research and Information Publication (ORIP) for the financial support in the publication of this research. Secondly, many thanks go to the various organizations and respondents who participated by responding to the questionnaires for the success of this study. Finally, many thanks go to my wife Siduduziwe and daughters Khanyisile and Nokukhanya who gave me most of their time to do this research. God bless you all.

References

[1] K. C Laudon, and J. P Laudon, "Management Information Systems-Managing the digital firm". 8th ed. India: Prentice Hall 2004.

[2] C. E. Lucier, and J. D Torsilieri, "Analysing Requirements and Defining Microsoft.net Solution Architectures: E-Business Microsoft Corporation", Microsoft Press 2002.

[3] K. E. Kendal, and J. E. Kendal, "Systems Analysis and Design". 5th ed. India: Prentice Hall.2004.

[4] J. A. O`Brien, "Introduction to Information Systems". 12th ed. Irwin: McGraw-Hill 2005.

[5] M. Stamp, "Information Security: Principles and Practice". USA: John Wiley &Sons Inc 2005.

[6] F. Warwick, "Computer Communications Security: Principles, Standard Protocols and Techniques. USA: Prentice Hall. 1994.

[7] T. R. Peltier, "Information Security Risk Analysis". USA: Auerbach Publications 2001.

[8] S. Petterson, "Database and network", An International Journal of Database and network practice, vol.38, 2008, pp.9-23.

[9] T. P Layton, "Information Security: Design, Implementation, Measurement, and Compliance". USA: Auerbach Publications 2006.

[10] S. Lomash, and P. A Mishra, "Business Policy and Strategic Management". New Delhi, India: Vikas Publishing House (Pvt) Ltd 2005.

[11] G. H. Wold, "Disaster recovery planning process", Disaster recovery Journal. Vol. 5 #1, 1997. Retrieved June 30, 2013, from Web site: http://www.drj.com/new2dr/w2_002.htm

[12] Federal Emergency Management Agency, "IT Disaster Recovery Plan". Retrieved June 30, 2013, form Web site: http://www.ready.gov/business/implementation/IT 2012 .

[13] http://www.smecd.gov.zw/index.php/sme-funding-facilities.

[14] http://www.gta.gov.zw/index.php/ministries/ministry-of-small-and-medium-enterprises.

[15] S. Alter, "Information Systems - A Management Perspective". 2nd ed. USA: The Benjamin 1996.