

language are also “read” both by the interviewee as well as the interviewer.

Questionnaires are a good way of collating data and information swiftly (Bell, 1993).

The aim of the questionnaire was to:

- ascertain whether the solutions suggested by the literature would be beneficial
- collate the data and find commonalities
- keep the interview process consistent and effective

Qualitative data collection utilizes rich and diverse data to answer questions and variability and complexity of human life. Table 8 below illustrates six different sources of evidences Yin (2003).

Table 8: Data Collection Methods (Yin, 2003)

Source	Method	Comments
Documents	Communiqués and written reports Administration documents Formal studies or evaluations Newspaper and articles from the mass media	This kind of information is likely to be relevant to every case study topic
Archival records	Service records Organisational records Maps, charts and lists Survey data and personal records	Often in computerised form
Interviews	Open-ended nature Focused Survey	The most important and essential source of case study information

Direct observation	Formal data Casual data	
Participant-observation	Being resident in a neighbourhood Functional roles in a environment Staff member in an organisational setting Being a key decision maker	Special mode of observation where the investigator is not a passive observer
Physical artefacts	Technological device Tool or instrument A work of art Other physical evidence	Less relevant potential in most typical kind of case study

A questionnaire is a series of written questions on a topic about which the subjects' opinions are sought (Sommer & Sommer, 2001). Questionnaires can be self-administered, that is

- When people answer a questionnaire they have received in the mail or at some event.
- When people are asked questions by an interviewer and people answer the questions openly.

The most difficult aspect about a questionnaire is its construction and the interpretation of the results.

Because there are many ways to ask questions, the questionnaire is very flexible. Questionnaires should be developed and tested carefully before being used on a large scale. There are three basic types of questionnaires (Dawson, 2002):

- Closed ended Questionnaires
 - Closed ended questions include all possible answers/prewritten response categories, and respondents are asked to choose among them.
 - For Example is multiple choice questions and scale questions.

- Type of questions used to generate statistics in quantitative research.
- As these follow a set format, and most responses can be entered easily into a computer for ease of analysis, greater numbers can be distributed.
- Open-ended Questionnaire
 - Open-ended questions allow respondents to answer in their own words.
 - Open-ended questionnaires do not contain boxes to tick but instead leave a blank section for the respondent to fill in.
 - Where closed ended questionnaires might be used to find out how many people use a service, open-ended questionnaires might be used to find out what people think about a service.
 - As there are no standard answers to open-ended questions, data analysis is more complex.
 - As opinions are being sought and not statistics, fewer questionnaires need to be distributed.
- Combination of both closed and open-ended questionnaires may allow one to find out how many people use a service and what they think of the service in the same form. Alternatively, a questionnaire begin with a series of closed – ended questions, with boxes to tick or scales to rank, and then finish with a section of open-ended questions or more detailed responses.

For this study an open-ended questionnaire was distributed to the Risk and BCP Managers of each of the four participating companies. The questionnaire, (See Appendix A – Research Questionnaire), was emailed to all the selected participants prior to the interview.

The basis and origin for the open-ended questionnaire is displayed in the table below.

Table 9: Questions, Basis and Origin

Questions	Basis for Question	Origin
1. Does the company have a written business continuity	To establish whether the company has a BCP in place, as this is a	Section 2.2

plan?	prerequisite for the company that is interviewed.	
2. Where is the company's BCP kept and who has access to this document?	How accessible is this document? Are employees allowed access it when necessary.	Section 2.4.2
3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?	To determine whether every disaster or threat was considered	Section 2.3
4. Does the DRP form part of the BCP or is it a separate plan altogether?	To determine whether the DRP is part of the BCP or a separate plan altogether	Section 2.2
5. Does business continuity and disaster recovery readiness have the support of top management in your organization?	If top management does not support the plan, this might possibly be a reason for BCP failure	Section 2.2
6. What happens if key personnel are not available during a disaster?	To determine whether the company is solely dependent on key personnel or whether alternative options are available. The answer to this question will identify the level of risk	Section 2.4.2
7. Has your organization identified which vendors may need	To determine whether this part within the plan has been considered as this	Section 2.4.1

access to your facility after a disaster?	could also lead to prolonged downtime.	
8. How often is the BCP reviewed or updated?	This is one of the most important points to the success of a BCP.	Section 2.4.1
9. How are business critical applications identified?	This question is to determine how critical applications are identified.	Section 2.2
10. Who is responsible for identifying these applications?	This question is to determine whether decisions are only from an IT perspective or whether the business owner is involved as well.	Section 2.2
11. Was your disaster covered by your plan, if no, why?	This question is to determine whether any of these disasters were covered.	Section 2.1
12. Do you perform back-ups faithfully and include every server and hard disk?	If a critical server or application is omitted this too can contribute towards prolonged recovery time or cause inability to recover at all.	Section 2.2
13. How often do you perform a BCP test? When tested, what were the results?	A major cause of BCP failure is when tests aren't performed regularly enough or when the tests do not include new applications and servers.	Section 2.4.1
14. Do you have unscheduled BCP	Unscheduled tests will keep the company aware	Section 2.4.2

test? If tested, did you pass your test?	and alert at all times so that those involved are familiar with the drill	
15. Does the company BCP highlight what are acceptable downtimes after specific disasters?	This question is to establish whether the company had highlighted specific downtime based on specific disasters and whether the Risk manager feels that these times are acceptable.	Section 2.4.1
16. Do you feel that these times are attainable?	To determine whether the downtime placed within SLAs are acceptable and attainable	Section 2.1
17. What was the impact of the disaster on business?	To establish whether income was lost or what other impact business suffered due to the severity of the disaster.	Section 2.4.1

Personal face-to-face interviews were conducted and a semi-structured questionnaire to keep the interviewer and interviewee focused and aligned with the research questions and objectives. Each interview lasted 30 to 40 minutes and was conducted at the premises of each of the companies. A digital recording device was used to record each interview. The Risk Manager or BCP Manager from each of the four companies within the Western Cape, who each had BCP in place, but still experienced prolonged downtime during a disaster were interviewed.

In conclusion, this chapter has formed an integral part of this study and described the research strategy, design, methods and techniques used to obtain the final results.

CHAPTER 5: DATA ANALYSIS AND FINDINGS

This chapter will display the outcome of the interview analysis and discuss the findings as well as the case study of each company's disaster which led to this research. The purpose of the interviews was to determine why companies experienced prolonged downtime during a disaster event. The data collected was analysed based on all interviewee responses which is also available on digital recording.

5.1 Data Analysis

According to Hancock (2002) data analysis is the process of summarizing and presenting all data collected in a way that presents the most important features. Hancock is also of the opinion that in qualitative research different techniques are used to discover the bigger picture such as

- Transcribing which is the process of writing down everything while conducting the interview or that was recorded during the interview.
- Content analysis which refers to the process of interpreting the data collected.
- Tape analysis which entails the process of replaying the recorded interview to analyze the data rather than transcribing.

Seidel (1998) is of the opinion that analysing qualitative data is a simple process that consists of three simple steps as shown in Figure: 12

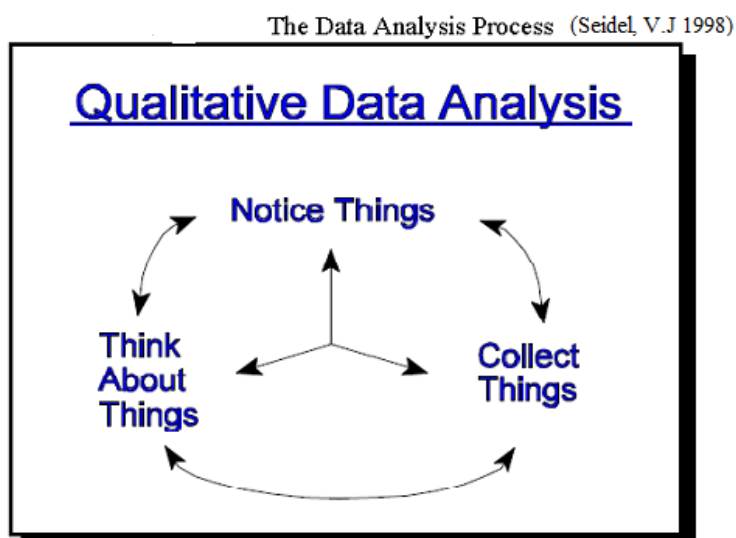


Figure 12: The Data Analysis Process

1. Noticing things means making observations, writing field notes, tape recording interviews and gathering documents in order to produce a record of things that you have noticed.
2. Collecting things is similar to putting the pieces of a jig-saw puzzle together. After noticing and naming the data, the next step is to sort the data to determine what would be useful to the research study.
3. Thinking about things is the process of examining the things you have collected. Your goals are to make sense out of each collection, look for patterns and relationships both within a collection, and also across collections and make general discoveries about the phenomena being researched.

Processing and analysing data involves a number of closely related operations which are performed with the purpose of summarizing the collected data and organizing these in such a manner so as to answer the research questions (Dawson, 2002).

The Data Processing operations are:

1. Editing- a process of examining the collected raw data to detect errors and omissions and to correct these when possible.
2. Classification- a process of arranging data in groups or classes on the basis of common characteristics, depending on the nature of phenomenon involved
 - 2.1 Classification according to attributes: here data is analysed on the basis of common characteristics which can either be:
 - 2.1.1 Descriptive such as literacy, sex, religion and so on
 - 2.1.2 Numerical such as weight, height, income etc.

The researcher must ensure that the data is converged in an attempt to understand the overall case, not the various parts of the case, or the contributing factors that influence the case (Baxter & Jack, 2010).

5.1.1 Data Analysis using a computer program

Qualitative researchers often find themselves overwhelmed by the amount of data and in need of tools to extend their human senses (Meyer & Avery, 2008). This has led the development of a number of software packages designed for this purpose. An often overlooked option is Microsoft Excel. Excel is generally

considered a number cruncher. However its structure and data manipulation and display features can be utilized for qualitative analysis.

Microsoft Excel was used as a data analysis tool for this study. Responses for each company were entered into an Excel spreadsheet, next to each question from the open-ended questionnaire. In this way the response for each company was displayed on a separate Excel spreadsheet. Data was analyzed by entering the responses of each respondent and creating columns marked Company A to Company D representing each of the four companies that participated in the research as illustrated in Appendix B. Common answers were grouped together for each company.

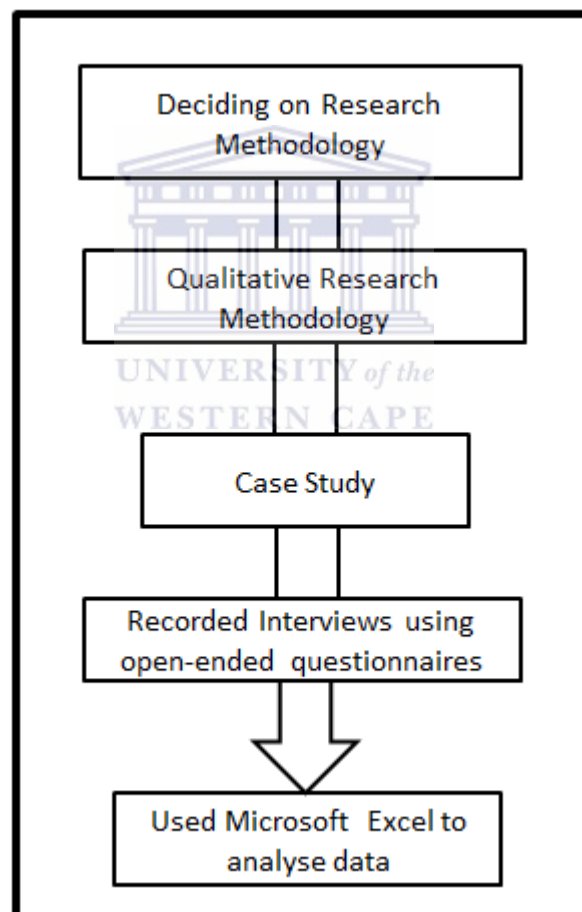


Figure 13: Research Process

The above process (Figure 13) was used to obtain the objective of this study which is why do companies that have BCP in place still experience prolonged downtime during a disaster. The above process was followed for each of the four companies so

that the original focus which is why do companies that have BCP in place and perform regular testing still experience prolonged downtime during a disaster is maintained. The findings attained through the research process are presented in this chapter

Before embarking on the research project a Non-Disclosure Agreement (NDA) with each company that was interviewed had to be signed. It was agreed that none of the companies or their employees would be mentioned in this research paper.

The Risk Manager or BCP Manager from each of the four companies that are based in the Western Cape was interviewed. Each of the companies has BCP in place, test it regularly but still experience prolonged downtimes during a disaster.

5.2 Findings - Case Studies

In order to protect the companies and participants, they will be referred to as Company A to D. Their stories are as follows:

5.2.1 Finding of Case Study 1 (Company A)

5.2.1.1 Introduction to Company A

Company A is one of South Africa's largest outdoor retail stores, with more than one hundred branches all over South Africa as well as in Namibia and Botswana. They are considered a well-established and reputable retail outlet in South Africa's retail market. The company employs about 1000 to 1500 permanent and casual staff nationally. About 500 of these permanent employees stationed at the Head Office alone. Each branch is equipped with the latest computer terminals on which the Point of Sale (POS) software is installed. These computer terminals connect to a computer known as the back office terminal which is situated in the store manager's office. The back office terminal for each store constantly communicates with the servers at Head Office to report back sales transactions, stock levels of each item, credit card transactions and so on. If a server "goes down" meaning that either the server crashed or the network lines between a store and the Head Office are not operational, that store is "shut out" electronically to the outside world and has to

trade manually. This means that staff members within the store have to write down each cash transactions in an invoice book. No debit or credit card transactions are allowed, and in today's age that is an imperative part of every business as most patrons use their debit or credit cards.

5.2.1.2 Disaster of Company A

On the 20th of September 2011 the company's Head Office in Cape Town experienced a power failure. Although the Datacentre is equipped with an Uninterrupted Power Supply (UPS), it only lasted for 10 minutes which was just enough time to allow the system administrator to shut-down all servers. All 220 VAC power equipment such as servers, network switches, routers and other electronic equipment were now non-operational. Communication between all stores and Head Office was down, thereby causing stores to be electronically "shut out", thus causing sales staff within the stores to write down each cash transactions in an invoice book as no debit or credit card transactions could be processed.

The impact of the disaster on business was as follows:

- All stores had to trade manually and turn away customers that wanted to purchase items using a debit or credit card.
- No bookings or reserving of items for customers were available.
- Checking for a particular item at a different branch for customers was not possible.
- Most of the staff at Head Office was unable to perform their duties until the power was restored as everyone relied on various systems to perform daily tasks.
- The power failure lasted for 4 hours, which is an extremely long time for any retail company.

After interviewing the Risk Manager it was established that the company overlooked the fact that they would ever experience a power failure seeing that the company is on the same power substation as parliament. The company had therefore made no provisions or alternatives for the event of a power failure.

This decision had proved to be catastrophic. As previously stated a disaster of this magnitude can definitely cause both financial and reputability damage.

The table below provides a summary of the questions answered by the Risk Manager.

Table 10: Summary of answers (Company A)

Questions	Answers
1. Does the company have a written business continuity plan?	Yes
2. Where is it kept and who has access to this document?	Kept on SharePoint for the whole company to view, as well as in the IT department and at the DR Site
3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?	Yes, lack of additional personnel. We have exclude events such as floods, tornadoes and so on. Non critical business applications due to budget constraints. Power failures as company is on the same sub-station as parliament and the chances that parliament would experience a power failure is very slim. Not sufficient business and technical staff involve in the plan
4. Does the DRP form part of the BCP or is it a separate plan altogether?	The DRP is part of the BCP
5. Does business continuity and disaster recovery readiness have support of top management in your organization, if no why?	Yes, There is a committee that monitors all the BCP tests. Top management does not fully understand the importance of BCP
6. What happens if key personnel are not available during a disaster?	Our BCP and DR is managed by a third party who has the necessary resources to assist when key personnel is not

	available
7. Have your organization identified which vendors may need access to your facility after a disaster?	Yes only for specific vendors
8. How often is the BCP reviewed and updated?	We do our testing every 6 months and generally this is when we update our plan, as we test our application changes in the test as well.
9. How is business critical applications identified?	Through general consciences among IT and Business. No specific Business Impact Analysis Tools
10. Who is responsible for identifying these applications?	IT and Business
11. Was your disaster covered by your plan, if no why?	No, our company shares the same sub-station as parliament and the chances that parliament would experience a power failure is very slim. This factor was taken for granted.
12. Do you perform back-ups faithfully and include every server and hard disk?	No, budget constraints due to the size of data that will be saved to disk. Disks are expensive. Test servers. Non critical business applications. All business critical servers are backed up on a daily basis.
13. How often do you perform a BCP test? If tested, did you pass your test?	Every 6 months. No not all the time, but then again that it the purpose of a BCP test to identify our shortcomings.
14. Do you have unscheduled BCP test? If yes, did you pass your test? If no, why?	No, too expensive. Testers need to be arranged before the time.
15. Does the company BCP highlight what are acceptable downtimes?	It was agreed by auditing committee that there is a recovery window for BC

	purposes.
16. Do you feel that these times are attainable?	Yes, we are currently comfortable with the time allocated.
17. What was the impact of the disaster on business?	SLA was missed with business. Retail outlet had to trade manually as databases resides at head office. No stock updates were sent to and fro from retail outlet. Only cash transactions.

The answer to question 11 in Table 10 above is an indication that the company took the power factor for granted, even though in Section 2.4 in the Literature review chapter, where Semer (1998) defines that power failures are one of the most common disaster that a company can experience.

Questions 2, 5, 6, 8, 9, 13 & 15 in the above table are specifically linked to the key elements of an effective BCP as depicted in Section 2.1.3 of the literature review chapter. The purpose for these questions was to determine whether Company A had applied the key elements of a BCP.

Table 11 below is an analysis of the answers to the questions that relates to the key elements of an effective BCP as per Section 2.1.3 of the Literature Review Chapter.

Table 11: Analysis of Company A's responses to research question linking to BCP Elements

Questions	Responses	Comply with key elements of an effective BCP as per Section 2.1.3
2. Where is the company's BCP kept and who has access to this document?	Kept on SharePoint for the whole company to view, as well as in the IT department and at the DR Site	Before a plan can be tested, employers and employees need to be familiar with the content of the plan and their role in the response and recovery. This can be done by reading through the plan

		together and discussing how you would apply it to a fictional scenario.
5. Does business continuity and disaster recovery readiness have support of top management in your organization?	Yes, There is a committee that monitors all the BCP tests. Top management does not fully understand the importance of BCP	Get senior management involved and keep them committed.
6. What happens if key personnel are not available during a disaster?	Our BCP and DR is managed by a third party who has the necessary resources to assist when key personnel is not available	In order for a plan to succeed, there must be multiple agency cooperation and involvement.
8. How often is the BCP reviewed and updated?	We do our testing every 6 months and generally this is when we update our plan, as we test our application changes in the test as well.	Keep the plan current – Update the plan as applications gets updated
9. How are business critical applications identified?	Through general consciences among IT and Business. No specific Business Impact Analysis Tools	Identify critical businesses and supporting functions and perform business impact analyses.
13. How often do you perform a BCP test? When tested, what were the results?	Every 6 months. No not all the time, but then again that it the purpose of a BCP test to identify our shortcomings.	Test the business recovery process and evaluate test results
15. Does the company BCP highlight what are	It was agreed by auditing committee that there is a	Identify your recovery point objective (RPO) and

acceptable downtimes?	recovery window for BC purposes.	recovery time objective (RTO), making sure your data protection solutions can meet these requirements.
-----------------------	----------------------------------	--

The answers to questions 2, 5, 6, 8, 9, 13 & 15 in Table 11 above is an indication that Company A conformed to some of the key elements of an effective BCP.

5.2.2 Findings of Case Study 2 (Company B)

5.2.2.1 Introduction to Company B

This company provides multi-jurisdictional legal, tax, fiduciary, investment and fund administration services to private, corporate and institutional clients. They provide the highest levels of expertise and competence and work in a way that is uniquely personal, proactive and responsive. The firm currently employs over 550 employees with 12 offices across Europe, the Caribbean and South Africa. It has over \$125 billion worth of international assets under its administration. They have a deep understanding of multiple jurisdictions and industries, which has earned them various international accolades and the loyalty of their clients, many of whom have been with them for decades. Their private clients are families and individuals, entrepreneurs and senior business executives, whereas their corporate clients comprise of blue-chip corporations, listed and non-listed entities and multi-nationals and their institutional clients are fund managers from large, medium and small companies.

Being a financial institution requires that the company offer support 24/7 throughout the year to all its clients. The firm also acts as an outsourced company to various financial houses by administering all the clients' financial profiles. The SLA between the firm and these financial houses are that:

- There will be 100% uptime, allowing the financial houses to update the records of new and existing clients.
- Clients have 24 hours 7 days a week access to their investments and financial information.

- Clients of the financial houses are allowed to change or alter their investment profiles at any given time.

These SLA's are the core business of the company and the company thrive on its reputable and committed reputation to gain market share within this industry.

5.2.2.2 Disaster of Company B

The company has a web portal that allows all clients to check the status of their investments and also allows them to change their portfolio based on market reactions. The web portal is connected to a primary router that links into the Multiprotocol Label Switching (MPLS) and a secondary router that links to their disaster recovery site. The primary router connects the entire company both locally and internationally to its different divisions and to its clients. If for some reason this primary link fails there should be an automatic fail over the secondary link without any down-time or impact on business. The primary link failed on 14th July 2011. After an hour of investigating the network administrator discovered that the fail over to the secondary link did not occur automatically. He then manually switched over to the secondary link, only to discover that the router is not configured correctly and that no one within the IT department knows the correct configuration, as that router is the responsibility of an Internet Service Provider (ISP) company. The race was between the ISP and the network administrator to get either of the routers up. It took the network administrator four hours to reconfigure the primary router, whilst the ISP was still battling with configuring the secondary router.

After interviewing the company's Security and Risk manager it was discovered that the routers were overlooked and was never included in the BCP test. The company focused mainly on the actual servers and software that resides within the servers and not on the peripherals around the servers.

Due to the fact that trading and pricing updates could not be done, the impact of the disaster had been mainly financial as SLA's were not met. The company's reputation also suffered some damage.

Table 12 below is a summary of the answers of the Security and Risk manager for Company B

Table 12: Summary of answers (Company B)

Questions	Answers
1. Does the company have a written business continuity plan?	Yes
2. Where is it kept and who has access to this document?	Kept on SharePoint for the whole company to view. The complete IT department. At the Disaster Recovery Site.
3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?	Yes, lack of additional personnel. Not sufficient business and technical staff involve in the plan.
4. Does the DRP form part of the BCP or is it a separate plan altogether?	The DRP consist within the BCP.
5. Does business continuity and disaster recovery readiness have support of top management in your organization, if no why?	Yes
6. What happens if key personnel are not available during a disaster?	Vendors are on standby to assist. Support from vendors. There is an agreement with third party vendors for technical support in the event of a disaster.
7. Have your organization identified which vendors may need access to your facility after a disaster?	Yes only for specific vendors.
8. How often is the BCP reviewed and updated?	Annually. Real time replication, that allows all new applications to be included automatically.
9. How is business critical applications identified?	By the use of a matrix. A Business Impact Analysis Tool is used to determine the impact of each application.

10. Who is responsible for identifying these applications?	Each business unit will sign off on their own application.
11. Was your disaster covered by your plan, if no why?	No, there was no connectivity.
12. Do you perform back-ups faithfully and include every server and hard disk?	No, test servers. Non critical business applications. All business critical servers are backed up on a daily basis. Real time replication.
13. How often do you perform a BCP test? If tested, did you pass your test?	Every 6 months. We do not pass all the time. Once a year an ICT test is performed. This is a technical test to ensure that we are able to restore all servers. A user test is done once a year to ensure that all applications restored are fully operational.
14. Do you have unscheduled BCP test? If yes, did you pass your test? If no, why?	No, Company is not ready for it. Yes would like to do unscheduled tests.
15. Does the company BCP highlight what are acceptable downtimes?	Yes, form part of the BIA.
16. Do you feel that these times are attainable?	Yes.
17. What was the impact of the disaster on business?	SLA was missed with business. Clients could not trade. Financial impact. Possibility of losing clients.

The answers to question 11 in Table 12 above highlight that Company B did not perform a proper analysis of all its equipment, thereby causing them to overlook a router which is pertinent to their daily operations.

Questions 2, 5, 6, 8, 9, 13 & 15 in the above table are specifically linked to the key elements of an effective BCP as depicted in Section 2.1.3 of the literature

review chapter. The purpose for these questions was to determine whether Company B had applied the key elements of a BCP.

Table 13 below is an analysis of the answers to the questions that relates to the key elements of an effective BCP as shown in Section 2.1.3 of the Literature Review Chapter.

Table 13: Analysis of Company B's responses to research question linked to BCP Elements

Questions	Responses	Comply with key elements of an effective BCP as per Section 2.1.3
2. Where is the company's BCP kept and who has access to this document?	Kept on SharePoint for the whole company to view. The complete IT department. At the Disaster Recovery Site.	Before a plan can be tested, employers and employees need to be familiar with the content of the plan and their role in the response and recovery. This can be done by reading through the plan together and discussing how you would apply it to a fictional scenario.
5. Does business continuity and disaster recovery readiness have support of top management in your organization?	Yes	Get senior management involved and keep them committed.
6. What happens if key personnel are not available during a disaster?	Vendors are on standby to assist. Support from vendors. There is an agreement with third party vendors for technical	In order for a plan to succeed, there must be multiple agency cooperation and involvement.

	support in the event of a disaster.	
8. How often is the BCP reviewed and updated?	Annually. Real time replication, that allows all new applications to be included automatically.	Keep the plan current – Update the plan as applications gets updated
9. How are business critical applications identified?	By the use of a matrix. A Business Impact Analysis Tool is used to determine the impact of each application.	Identify critical businesses and supporting functions and perform business impact analyses.
13. How often do you perform a BCP test? When tested, what were the results?	Every 6 months. We do not pass all the time. Once a year an ICT test is performed. This is a technical test to ensure that we are able to restore all servers. A user test is done once a year to ensure that all applications restored are fully operational.	Test the business recovery process and evaluate test results
15. Does the company BCP highlight what are acceptable downtimes?	Yes, form part of the BIA.	Identify your recovery point objective (RPO) and recovery time objective (RTO), making sure your data protection solutions can meet these requirements.

The answers to questions 2, 5, 6, 8, 9, 13 and 15 in Table 13 above, highlighted that most of the key elements of a BCP had been adhered to by Company B.

5.2.3 Findings of Case Study 3 (Company C)

5.2.3.1 Introduction to Company C

Company C is an African mobile communications company providing voice, messaging, data and converged services to over 45 million customers. From their roots in South Africa, they have grown their operations to include networks in Tanzania, the Democratic Republic of Congo ('DRC'), Mozambique and Lesotho. They also provide carrier and business services to customers in over 70 countries.

This company is one of the world's largest mobile communications companies that is currently listed on the JSE. Even though their Head Office is based in Johannesburg the company's technical stronghold is in Cape Town.

On a daily basis the service desk in Cape Town receives numerous calls from old and new subscribers, distributors and vendors for information, product updates and information. It is therefore imperative that all systems have a 100% uptime, allowing users to access information whenever from wherever as well as permitting vendors and agents to sign up new subscribers or upgrade available contracts. If the system goes down or users, vendors, agents and distributors aren't able to access the system, no information of a particular user is available and no new contracts can be activated or existing contracts upgraded. This could have disastrous repercussions on the reputation of the company and might cause them to lose market value meaning a loss in revenue.

5.2.3.2 Disaster of Company C

On Saturday the 25th of August 2012 applications across multiple system platforms in Cape Town sporadically stopped functioning. Every client accessing the company's portal could not access, read, update or cancel information as the system would intermittently block access to the database server. Each scenario is listed as part of the BCP strategy, thereby informing

the operator in the service department what to do in the event something happens; this scenario however was not listed. The operator did what he thought was a logical approach by rebooting the system every time in the hope that the system would reset itself. The telephones at the service desk rang all day from frustrated vendors as most of their patrons would walk out of the store causing a loss in revenue. After half the day had passed, the service desk operator decided to escalate the matter. Immediately the system administrator, network administrator and database administrator rushed to the Cape Town office. Seeing that the problem was intermittent it made diagnosing very difficult for the technical team, but after nearly two hours of investigation it was discovered that one of the application services would automatically restart itself. The system administrator immediately put alerts in place that should any of the services fail an email be sent to the appropriate parties concerned.

The interview with the Risk Manager revealed that the monitoring of the application services had been overlooked, and therefore was not listed in the BCP strategy documents that are given to service desk operators.

Seeing that the system was down for eight hours nationally, distributors and vendors had to turn away new and existing customers as they could not access the main server. This certainly had a great financial impact on the company and also damaged its reputation.

Table 14 below is a summary of the answers given by the Risk Manager for Company C.

Table 14: Summary of answers (Company C)

Questions	Answers
1. Does the company have a written business continuity plan?	Yes
2. Where is it kept and who has access to this document?	Kept on SharePoint for the whole company to view.
3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?	No, everything is covered.

4. Does the DRP form part of the BCP or is it a separate plan altogether?	The DRP is part of the BCP. The BCP covers all the natural disasters. The DRP within the BCP covers the technical aspects.
5. Does business continuity and disaster recovery readiness have support of top management in your organization, if no why?	Yes, there is a Business Continuity Management (BCM) team that looks after enterprise wide BCP.
6. What happens if key personnel are not available during a disaster?	Vendors are on standby to assist. Support from vendors. All key personnel have alternative numbers from a different service provider. All critical services have standby and escalation procedures in place.
7. Have your organization identified which vendors may need access to your facility after a disaster?	Yes only for specific vendors. Service Level Agreements (SLA) is in place with specific vendors.
8. How often is the BCP reviewed and updated?	Every 6 months. Real time replication, that allows all new applications to be included automatically. Some critical applications are reviewed quarterly.
9. How is business critical applications identified?	By the use of a matrix. All business critical services and systems are rated as per criticality. (Mission critical, business critical, non-critical).
10. Who is responsible for identifying these applications?	Business owner. BCM Team.
11. Was your disaster covered by your plan, if no why?	No, We did not consider monitoring any services as we are already monitoring the software.
12. Do you perform back-ups faithfully and include every server and hard disk?	No, test servers. Non critical business applications. All business critical servers are backed up on a daily basis. Real time

	replication.
13. How often do you perform a BCP test? If tested, did you pass your test?	Every 6 months. No we do not pass all the time. Some applications are tested quarterly. Insufficient disk space on server.
14. Do you have unscheduled BCP test? If yes, did you pass your test? If no, why?	No.
15. Does the company BCP highlight what are acceptable downtimes?	Yes, Uptime is 99%.
16. Do you feel that these times are attainable?	Yes, Time frames has been thoroughly tested and agreed upon. Due to the nature of our business we need to be up all the time.
17. What was the impact of the disaster on business?	Possibility of losing clients. Entire call centre was down. Reputation was damaged


The answer to question 11(in bold) in Table 14 above proved that not only should the software be monitored, but also the application as well as services of any application.

Questions 2, 5, 6, 8, 9, 13 & 15 in the above table are specifically linked to the key elements of an effective BCP as depicted in Section 2.1.3 of the literature review chapter. The purpose for these questions was to determine whether Company C had applied the key elements of a BCP.

Table 15 below is an analysis of the answers to the questions which relate to the key elements of an effective BCP as shown in Section 2.1.3 of the Literature Review Chapter.

Table 15: Analysis of Company C's responses to research question linking to BCP Elements

Questions	Responses	Comply with key elements of an effective BCP as per Section 2.7
2. Where is the company's BCP kept and who has access to this document?	Kept on SharePoint for the whole company to view.	Before a plan can be tested, employers and employees need to be familiar with the content of the plan and their role in the response and recovery. This can be done by reading through the plan together and discussing how you would apply it to a fictional scenario.
5. Does business continuity and disaster recovery readiness have support of top management in your organization?	Yes, there is a Business Continuity Management (BCM) team that looks after enterprise wide BCP.	Get senior management involved and keep them committed.
6. What happens if key personnel are not available during a disaster?	Vendors are on standby to assist. Support from vendors. All key personnel have alternative numbers from a different service provider. All critical services have standby and escalation procedures in place.	In order for a plan to succeed, there must be multiple agency cooperation and involvement.
8. How often is the BCP reviewed and updated?	Every 6 months. Real time replication, that allows all new applications to be included automatically. Some critical	Keep the plan current – Update the plan as applications gets updated

	applications are reviewed quarterly.	
9. How are business critical applications identified?	By the use of a matrix. All business critical services and systems are rated as per criticality. (Mission critical, business critical, non-critical).	Identify critical businesses and supporting functions and perform business impact analyses.
13. How often do you perform a BCP test? When tested, what were the results?	Every 6 months. No we do not pass all the time. Some applications are tested quarterly. Insufficient disk space on server.	Test the business recovery process and evaluate test results
15. Does the company BCP highlight what are acceptable downtimes?	Yes, Uptime is 99%. 	Identify your recovery point objective (RPO) and recovery time objective (RTO), making sure your data protection solutions can meet these requirements.

The answers to questions 2, 5, 6, 8, 9, 13 and 15 in Table 15 above highlights that most of the key elements of a BCP had been adhere to by Company C.

5.2.4 Findings of Case Study 4 (Company D)

5.2.4.1 Introduction to Company D

Founded in 1997, Company D is a privately owned Internet Service Provider (ISP), providing broadband internet access and hosting solutions across South Africa to both home and business customers in equal measure.

With over 30 000 subscribers enjoying their world-class network experience, this company has consistently been independently rated as one of the leading ISPs in South Africa. In 2006 the company won their first title as Best ADSL

Service Provider in South Africa and this meant that they had to uphold their reputation by providing 24 hours a day, seven days a week internet access to users nationally.

These customers are supported by 120 staff members, who spend every day trying to go beyond the call of duty, which is why the company is close to achieving their goal of becoming South Africa's most loved and trusted ISP.

Some of their customers require support between Limpopo to London. It is therefore imperative that the internet lines and network connectivity be up and running at all times as businesses and individuals are dependent on them for Webhosting, Internet Services, emails and so on. Companies in this type of industry rely on their reputation to gain market share.

5.2.4.2 Disaster of Company D

On the 16th of May 2012 the company lost network connectivity to the company that supplies them with bandwidth, and as a result all their clients could not connect to the internet. This meant that private as well as their business clients were unable to surf the net, check emails, perform online banking, download, whilst in addition businesses were not able to trade, communicate to their clients, and so on. The company battled the entire day with their supplier to get the line restored.

Even though their BCP covered all aspects of business the network connectivity between Company D and its bandwidth supplying company was overlooked. The company had since put in additional lines allowing immediate fail over in the event that one line goes faulty.

The BCP and Risk Manager highlighted the disastrous impact on the company's reputation as well as financial impact as many businesses had SLA's in place with their clients.

Table 16 below is a summary of the answers of the BCP and Risk manager.

Table 16: Summary of answers (Company D)

Questions	Answers
1. Does the company have a written business continuity plan?	Yes

<p>2. Where is it kept and who has access to this document?</p>	<p>Kept on SharePoint so that anyone in the company can access it. Key players. Senior managers.</p>
<p>3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?</p>	<p>Yes, Lack of additional personnel. Not sufficient business and technical staff involve in the plan. Location for staff to operate from.</p>
<p>4. Does the DRP form part of the BCP or is it a separate plan altogether?</p>	<p>The DRP within the BCP covers the technical aspects. Separate plans that makes up a BCP. DRP is covered by IT and Operations. BCP is enterprise wide.</p>
<p>5. Does business continuity and disaster recovery readiness have support of top management in your organization, if no why?</p>	<p>Yes, Top management just approve the budget, but aren't really concern about BCP. Top management does not fully understand the importance of BCP.</p>
<p>6. What happens if key personnel are not available during a disaster?</p>	<p>Nothing, there aren't any support from vendors. No support from any outsources companies. All applications are developed in house to meet business specific requirements therefore systems are unique to business.</p>
<p>7. Have your organization identified which vendors may need access to your facility after a disaster?</p>	<p>Yes only for specific vendors.</p>
<p>8. How often is the BCP reviewed and updated?</p>	<p>Real time replication, that allows all new applications to be included automatically. No formal review. BCP and DRP are treated as live documents and are updated as and when new requirements are presented.</p>
<p>9. How is business critical applications identified?</p>	<p>By the use of a scorecard. Owners of the application are responsible for the server on which the applications reside.</p>


10. Who is responsible for identifying these applications?	Manager of the department in which the application reside. Information and security team.
11. Was your disaster covered by your plan, if no why?	No, not really. We weren't able to effectively get hold of that particular vendor and we haven't identified the redundancy that we required, therefore it was not part of the plan
12. Do you perform back-ups faithfully and include every server and hard disk?	No, test servers. Real time replication.
13. How often do you perform a BCP test? If tested, did you pass your test?	Some applications are tested quarterly. Tests are performed on a departmental basis.
14. Do you have unscheduled BCP test? If yes, did you pass your test? If no, why?	Yes when new changes take effect.
15. Does the company BCP highlight what are acceptable downtimes?	Yes, uptime is 99%
16. Do you feel that these times are attainable?	Yes, Due to the nature of our business we need to be up all the time.
17. What was the impact of the disaster on business?	SLA was missed with business. Possibility of losing clients. Reputation was damaged.

The answers to question 11 in Table 16 above is an indication that Company D did not perform a proper analysis of all its equipment and peripherals, thereby causing them to overlook a network connection that was relevant to their daily operations and that of their clients.

Questions 2, 5, 6, 8, 9, 13 & 15 in the above table are specifically linked to the key elements of an effective BCP as depicted in Section 2.1.3 of the literature review chapter. The purpose for these questions was to determine whether Company D had applied the key elements of a BCP.

Table 17 below is an analysis of the answers to the questions which relate to the key elements of an effective BCP as shown in Section 2.1.3 of the Literature Review Chapter

Table 17: Analysis of Company D’s responses to research question linking to BCP Elements

Questions	Responses	Comply with key elements of an effective BCP as per Section 2.1.3
2. Where is the company’s BCP kept and who has access to this document?	“Kept on SharePoint so that anyone in the company can access it. Key players. Senior managers”. 	Before a plan can be tested, employers and employees need to be familiar with the content of the plan and their role in the response and recovery. This can be done by reading through the plan together and discussing how you would apply it to a fictional scenario.
5. Does business continuity and disaster recovery readiness have support of top management in your organization?	“Yes, Top management just approve the budget, but aren’t really concern about BCP. Top management does not fully understand the importance of BCP”.	Get senior management involved and keep them committed.
6. What happens if key personnel are not available during a disaster?	“Nothing, there aren’t any support from vendors. No support from any outsources companies.	In order for a plan to succeed, there must be multiple agency cooperation and

	All applications are developed in house to meet business specific requirements therefore systems are unique to business”.	involvement.
8. How often is the BCP reviewed and updated?	“Real time replication, that allows all new applications to be included automatically. No formal review. BCP and DRP are treated as live documents and are updated as and when new requirements are presented”.	Keep the plan current – Update the plan as applications gets updated
9. How are business critical applications identified?	“By the use of a scorecard. Owners of the application are responsible for the server on which the applications reside”.	Identify critical businesses and supporting functions and perform business impact analyses.
13. How often do you perform a BCP test? When tested, what were the results?	“Some applications are tested quarterly. Tests are performed on a departmental basis”.	Test the business recovery process and evaluate test results
15. Does the company BCP highlight what are acceptable downtimes?	“Yes, uptime is 99%”	Identify your recovery point objective (RPO) and recovery time objective (RTO), making sure your data protection solutions can meet these requirements.

--	--	--

The answers to questions 2, 5, 6, 8, 9, 13 and 15 in Table 17 above highlights that most of the key elements of a BCP had been adhere to by Company C.

5.3 Major Cause of Prolonged Downtime as per Company

Table 18 below is a summary of the primary reasons for the prolonged downtime during the respective disasters experienced by each of the four companies that were researched.

Table 18: Reasons for the prolonged downtime per company

Companies	Summary of reason of failure
Company A	The supply of electricity had been taken for granted and therefore never included it into the BCP.
Company B	The inclusion of routers was overlooked and therefore never tested.
Company C	All critical elements within an application were overlooked and not fully monitored therefore was never tested.
Company D	Redundancy for that connection was not identified or that network connection was overlooked .

If we consider the responses for each company in Table 18 above, there is a commonality in that most of the companies (company B to D) overlooked hardware peripherals namely a router and a network connection as well as software peripherals which is the service responsible for allowing an application to operate. To overcome the “overlooking” factor the companies that were researched should definitely consider incorporating another step in the Common BCP Process (Figure 8 in the Literature Review Section). This new step would include “identifying critical points of failure” and should include checking all aspects and include various software and hardware technical department heads that are responsible for their area of expertise. Each department head should then sign off his area and be involved in the testing phase of the Common BCP Process and signoff that their area

has been tested. The new step namely “identifying critical points of failure” would be incorporated between the “BIA” phase and the “Develop a BCP” in the Common BCP Process. The reasons for BCP failure is highlighted in table 18 and can contribute directly to the disaster events in section 2.4 of the literature review chapter.

In the following chapter we will look at a model that will assist these companies and possibly other companies in South Africa to have a reduced or no downtime during a disaster.



CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

The aim of this research was to determine why companies that had BCP in place still experienced prolonged downtime during a disaster. The extensive literature covered in chapter 2 highlights the different types of disaster events, key elements of an effective BCP and the factors that cause BCP failure.

Due to all the integrations of systems, most companies have come to realize that their business is now more dependent on IT than ever before and that greater focus should be placed on BCP to ensure that companies do not experience prolonged downtime during a disaster. Companies should strengthen their BCP and close any loop holes that might exist.

The companies that were studied and possibly many other companies that have a BCP in place, have realised that certain elements or criteria do not exist within their BCP thus causing them to experience prolonged downtime during a disaster.

Following the results of the research conducted with the four companies based within the Western Cape, it is evident that there is a vital gap within their BCP Process. If we compare the Common BCP Process as shown in Figure 14 below to that of BCP Process Model F Figure 15 below, it becomes apparent that an additional step has been added. This step is the step that was mentioned in the above Chapter in section 5.3 as “identifying critical points of failure”.

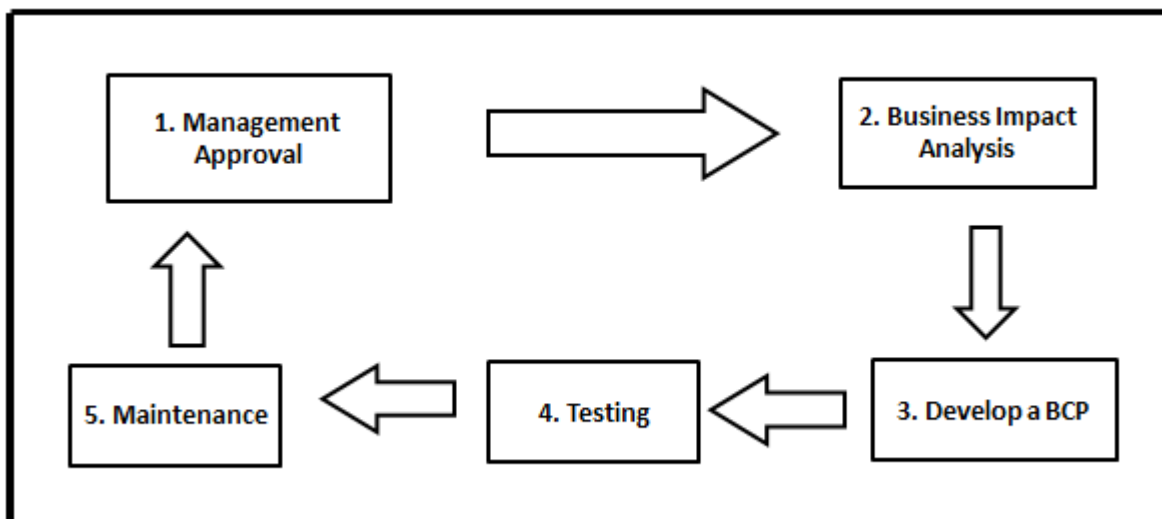


Figure 14: Common BCP Process

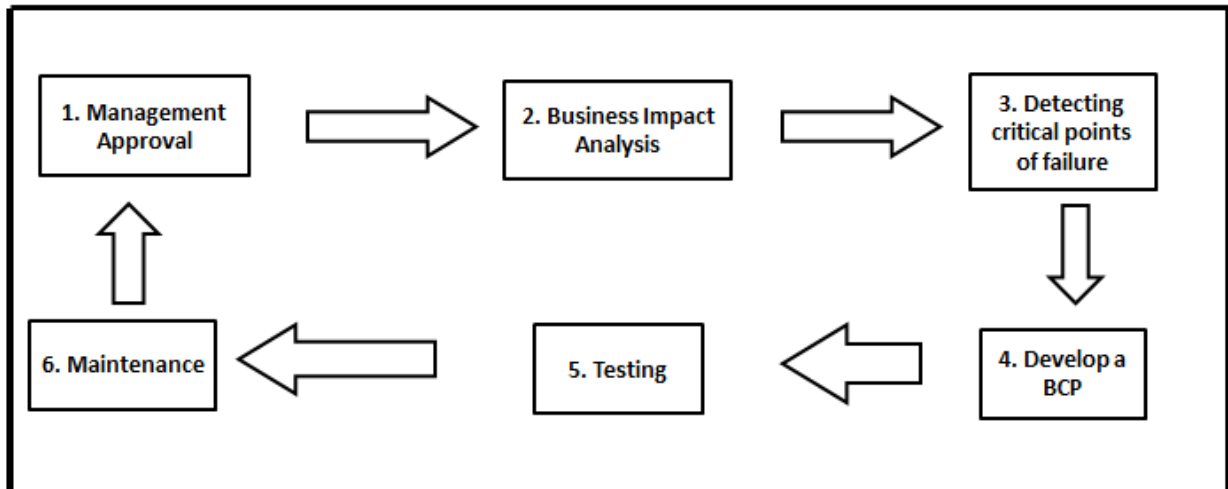


Figure15: Proposed BCP Process Model F

In addition point 3 “Detecting critical points of failure” should be expounded as follows:

1. Create a detailed architectural diagram highlighting each possible point of failure. This should be done on a software and hardware level, thus involving the Application Manager as well as the Technical Manager.
2. Identify, test and sign off on each point of failure based on the architectural diagram.
3. Rank and rate each point of failure, so that only significant points of failure are incorporated into the final BCP document.

It is with great expectation that once the missing step is incorporated that companies might have less if any downtime during a disaster. In summary, table18 highlights the key reasons for the prolonged downtime during a disaster event and figure 15 can assist companies in bridging the gaps in their BCP development.

6.1 Research Limitation

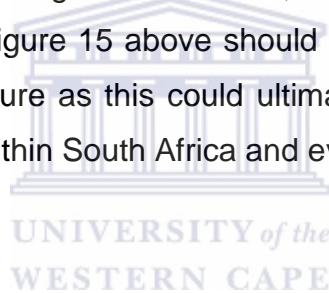
This study adopted a qualitative approach which resulted in subjective opinions of the individuals that were interviewed being formulated. The main limitation of this study is that most of the companies that were studied are based within the Western Cape. A further constraint is that only private and

public companies were studied and no NGO's and or Government Departments were involved. These limitations therefore allow a person to further investigate the scope of this research to the other provinces as well as studying NGO's and various Government departments.

6.2 Research Value

Many companies rely on the ability to conduct business continuously without missing any SLA's, as this could have a financial impact on them. Service orientated companies rely on their operations to have 99% uptime. Failing to do this, could result in their clients to seek a company that can offer them reliable and uptime service.

Table 18 in Chapter 5 proves that companies can experience prolonged downtime during a disaster by overlooking certain factors. In order to prevent companies from overlooking certain factors, it is therefore recommended that the additional step in Figure 15 above should be included in a common BCP process in future literature as this could ultimately improve BCP process for companies nationally within South Africa and even worldwide.



REFERENCES:

Aggelinos, G. & Katsikas, S.K. (2011). "Enhancing SSADM with disaster recovery plan activities" *Information Management & Computer Security*, pages 248-261

Aleem, A. and Antwi-Boasiako, A. (2011), "Internet auction fraud: the evolving nature of online auctions criminality and the mitigating framework to address the threat", *International Journal of Law, Crime and Justice*, September (special edition Fraud Management)

Alavi, M. & Carlson, P. (1992). "A Review of MIS Research and Disciplinary Development". *Journal of Management Information Systems*.

Aliaga, M. & Gunderson, B. (2002) "Interactive Statistics." [Thousand Oaks]: Sage

Al-Zahrani, A (2009) "Decision making assessment model throughout IT Business Continuity Planning (BCP) Lifecycle in small or medium-size organizations in Saudi Arabia" *Open University Malaysia*.

Babbie, E & Mouton, J. (2002). "The practice of social research". Cape Town: Oxford University Press.

Bajgoric, N & Moon, Y.B (2009) "Enhancing system integration by incorporating business continuity drivers" Vol. 109

Bateman, I, Authors, L, Albon, S, Balmford, A, Brown, C, Church, A, Haines-young, R, Jules, N, Turner, K, Vira & B, Winn, J (2011). "Conceptual Framework and Methodology"

Baxter, P. and Jack, S. (2010) "Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers" McMaster University, West Hamilton, Ontario, Canada

Bell, J. (1993). "Doing Your Own Research Project: A Guide for First-Time Researchers in Education and Social Science". Buckinghamshire, Open University Press.

Benbasat, I., Goldstein, D.K., Mead, M. (1997). "The Case Research Strategy in Studies of Information Systems". 11(3) : 369-386.

Botha, J. & Von Solms, R. (2004). "A cyclic approach to business continuity planning". *Information Management & Computer Security*. Vol 12 No. 4. 328-337.

Bless, C., & Higson-Smith, C. (1995). "Fundamentals of research methods. An African perspective". RSA: Juta.



Burns, N. & Grove, SK. (2005). "The Practice of Nursing Research: Conduct, Critique, and Utilization (5th Ed.)". St. Louis, Elsevier Saunders

Byrne, M (2001) "Ethnography as a qualitative research method" *AORN Journal*

Campbell, M. (2012). "Best Practices for Creating an Effective Business Continuity Plan" available on <http://esj.com/articles/2012/11/05/business-continuity-plan.aspx>

Camp, W. G. (2001). "Formulating and evaluating theoretical frameworks for career and technical education research". *Journal of Vocational Education Research*, 26 (1). Retrieved May 1, 2009 from: <http://scholar.lib.vt.edu/ejournals/JVER/v26n1/camp.html>

Cervone, H.F (2006). "Managing digital libraries: the view from 30,000 feet. Disaster recovery and continuity planning for digital library systems". OCLC Systems & Services. Vol. 22 No. 3. 173-178.

Chow, W.S. (2000) "Success factors for IS disaster recovery planning in Hong Kong". Hong Kong Baptist University, Hong Kong.

Chow, W. S and Ha, W. (2009) "Determinants of the critical success factor of disaster recovery planning for information systems". Journal: Information Management and Computer Security. Department of Finance and Decision Sciences, Hong Kong Baptist University, Kowloon Tong, Hong Kong, China

Clifton, R. (2000). "Business Continuity Planning" Occupational health & safety (Waco, Tex.)

Collis and Hussey (2003) "Business Research: A Practical Guide for Undergraduate and Postgraduate Students" Palgrave Macmillan, 2003

Creswell, JW. (1994). "Research Design: Qualitative & Quantitative Approaches". United States of America: Sage Publications.

Dawson, C. (2002), "Practical Research Methods", New Delhi, UBS Publishers' Distributors,

De Vos AS. & Fouche, CB. (1998). "General Introduction to Research Design, Data Collection Methods and Data Analysis". In De Vos (ed). Research at Grassroots. A primer for caring professions. Pretoria: Van Schaik Publishers.

Edwards, B (1994). "Developing a Successful Network Disaster Recovery Plan". Information Management & Computer Security, Vol. 2 No. 3, 1994, pp. 37-42 © MCB University Press , 0968-5227

Erickson, F. (1986). "Qualitative Methods in Research on Teaching". Wittrock (Ed.). New York: MacMillan.

Erlanger, L. (2006). "In case of emergency activate business continuity plan". InfoWorld. 27-31.79

Fade, S. (2004). "Using interpretative phenomenological analysis for public health nutrition and dietetic research: a practical guide". Proceedings of the Nutrition Society, (63): 647-653

Gardener, N.J.L. (2010) "Business Continuity Psychology - From Strategy to Benefits?"

Gerring, J. (2004). "What is a case study and what is it good for?" *The American Political Science Review*, 98 (2): 341-354.

Available at:

<http://ejournals.ebsco.com/direct.asp?ArticleID=PB1ADPV9TD9DTCRKJL0T>.

Glenn, J. (2002), "What is business continuity planning? How does it differ from disaster recovery planning?", Disaster Recovery Journal, available at: www.drj.com/articles/win02/1501-14p.html (accessed 11 May).

Gordon, C. (2000), "How to cost-justify a business continuation plan to management", Disaster Recovery Journal, available at: www.drj.com/articles/spring00/1302-05.html (accessed 7 March 2002).

Government of Canada Public and Safety. "A guide to business continuity planning" Retrieved on 2011-06-12 from <http://www.publicsafety.gc.ca/prg/em/gds/bcp-eng.aspx>

Grimaldi, R. (2002) "Why do Business Continuity Plans fail?" Journal: Risk and Insurance. Retrieved on 2011-10-20 from <http://www.rmmag.com/Magazine/PrintTemplate.cfm?AID=1483>

Hancock B, (2002), "Trent Focus for Research and Development in Primary Health Care: An Introduction to Qualitative Research." Trent Focus,

Harris, L. (2001). "Keeping IT alive when disaster strikes." Retrieved on 2011-08-12 from

http://www.itweb.co.za/index.php?option=com_content&view=article&id=44662&catid=116

Hearnden, K. (1995), "Business continuity planning: Part 4, Establishing business priorities", Computer Audit Update, vol. 8, pp. 3 - 13.

Hellman, L & Magnus, K (2008) "A Disaster Recovery Planning Guide- On how to mitigate the supply chain disruption risks of a totally destroyed central warehouse" Department of Fire Safety Engineering and Systems Safety Lund University, Swede. Report 5282

Heng, G. M (1996) "Developing a suitable business continuity planning methodology" FBCI, CDRP Group Manager, Standard Chartered Bank

Hudic, A., Islam, S., Kieseberg, P., Rennert, S., Edgar R. Weippl, (2013), "Data confidentiality using fragmentation in cloud computing", International Journal of Pervasive Computing and Communications, Vol. 9 Iss 1 pp. 37 - 51

Ingenuity (2006) "Success or Failure? Your Keys to Business Continuity Planning" © 2000-2006, Ingenuity, Inc. White Paper available at <http://www.teamingenuity.com/Sites/teamingenuity3/Documents/Technology/Ingenuity%20White%20Paper-%20Keys%20to%20BCP%20success.pdf>

Islam, S., Mouratidis, H. and Ju"rjens, J. (2011), "A framework to support alignment of secure software engineering with legal regulations", Journal of Software and Systems Modeling (SoSyM), Theme Section on Non-functional System Properties in Domain-Specific Modeling Languages (NFPinDSML), Vol. 10 No. 3, pp. 369-94

Kaplan, B. and Maxwell, J.A. (1994) ""Qualitative Research Methods for Evaluating Computer Information Systems," in Evaluating Health Care Information Systems:

Methods and Applications”, J.G. Anderson, C.E. Aydin and S.J. Jay (eds.), Sage, Thousand Oaks, CA, pp. 45-68.

Karakasidis, K. (1997). “A project planning process for Business Continuity.” KPMG Information Technology Consulting Division, Melbourne, Australia

Lee T (2009) “Using ITIL to measure your Business Continuity” Trinity Consulting Solutions LLC

Kohlbacher, F. (2005). “The use of qualitative content analysis in case study research”. Forum: Qualitative Social Research, Art. 21 (12/05). Available at: <http://www.qualitaqtive-research.net/fqs-texte/1-06/06-1-21-e.htm>

Lastrucci, C.L. (2002) “The Scientific Approach: Basic Principles of the Scientific Method” Science; Methodology, 257p

Imai, M., (1986), Kaizen. New York: McGraw Hill Publishing

Langley, E. (2010) “Business Continuity - Establish Recovery Point and Time Objectives” http://community.spiceworks.com/how_to/show/1676-business-continuity-establish-recovery-point-and-time-objectives

Levinson, V. (2012). “Disaster Recovery and Business Continuity Planning” Lesson we need to learn from Sandy. <http://blog.primetelecommunications.com/2012/11/12/disaster-recovery-and-business-continuity-planning-lessons-we-need-to-learn-from-sandy/>

Lindström, J., Samuelsson, S. & Hägerfors, A. (2010). “Business continuity planning methodology.” Disaster Prevention and Management, 19(2), pp.243-255. Available at: <http://www.emeraldinsight.com/10.1108/09653561011038039> [Accessed June 17, 2011].

Maslen, C. (1996). “Testing the plan is more important than the plan itself”. Business Recovery, Optus Communications

Marzanah A. J. (2009). "An investigation into methods and concepts of qualitative research in information research". *Computer and information science* 2 (4) Available at <http://www.ccsenet.org/journal/index.php/cis/article/view/3200/3714>

Mercer, V. N. (2001). "The double-edged sword: examining perceptions of technology as a process of enablement and construct within an academic organization". *Unpublished MA thesis*, University of North Carolina, October 2001.

Meyer, D.Z. & Avery L.M. (2008). "Excel as a Qualitative Data Analysis Tool" first published on September 20, 2008

Molinari, A (2010) "Top 10 Reasons Business Continuity and Disaster Recovery Plans Fail" *Business Continuity Management Professionals*

Moore, P (1995) "Critical elements of a disaster recovery and business / service continuity plan" Vol. 13, pp. 22 - 27

Morwood, G. (1998), "Business continuity: awareness and training programmes", *Information Management & Computer Security*, Vol. 6 No. 1, pp. 28-32.

Mouton, J. (1996). "Understanding social research". RSA: J.L van Schaik.

Mouton, J. (1998), "Patterns of Research Collaboration in Academic Science in South Africa". Lisbon, EASST.

Murphy E., Dingwall R., Greatbatch D., Parker S. & Watson P. (2007). "Qualitative research methods in health technology assessment: a review of the literature", School of Sociology and Social Policy, University of Nottingham, Nottingham, UK

Myers, M. D. 1994. A disaster for everyone to see: an interpretative analysis of a failed IS project. *Accounting, management and information technology*, 4(4): 185-201 Elsevier Science.

Myers, M.D. (2009) "Qualitative Research in Business & Management". Sage Publications, London

Neale, P., Thapa, S. & Boyce, C., (2006). "PREPARING A CASE STUDY : A Guide for Designing and Conducting a Case Study for Evaluation Input." Pathfinder International Tool Series, Monitoring and Evaluation – 1

Nickolette, C. and Schmidt, J. (2001) "Business Continuity Planning – Description & Framework". Business Continuity Planning white paper.

Nishchal, N. and Mathur, P. (2010), "Cloud computing: new challenge to the entire computer industry", Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference, pp. 223-8

Noakes-Fry, K. (2001) "Business Continuity and Disaster Recovery Planning and Management: Perspective" Technology overview

Pather, S. & Remenyi, D. (2005). Some of the philosophical issues underpinning research in Information Systems-form positivism to critical realism. South African Computer Journal, No 35.

Patton, E, Appelbaum, S.H. (2003). "The case for case studies in management research". *Management Research News*, 26(5): 60-71

Available at

<http://ejournals.ebsco.com/direct.asp?ArticleID=BDT0JKNLA89JLAQ51YCC>

Pit, M. & Goyal, S. (2004). "Business continuity planning as a facilities management tool". *Facilities*. Vol 22 No 3/4. 87-99.

Phelps, N. (1986). "Setting up a crisis recovery plan". *The Journal of business strategy*

Planning , B (2000). "Introduction to Business Continuity Planning". SANS Institute InfoSec Reading Room.

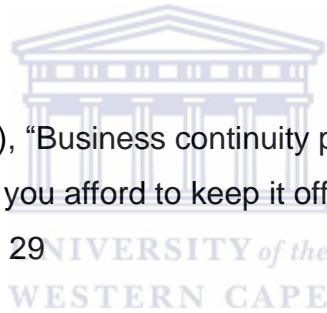
Priest, H. & Roberts, P. (2010). "Gathering and making sense of words". In Roberts, P. and Priest, H. (2010) Healthcare research A handbook for students and practitioners, Wiley-Blackwell, UK [Scholar Google e-book]. Rapoport, R.N.(1970) "Three Dilemmas in Action Research", Human Relations (23:6), pp. 499-513.

Proofpoint (2010), "Outbound email and data loss prevention in today's enterprise", Tech. Report, Proofpoint.

Rosenberg, N. (2010). "10 Steps to Implement a Disaster Recovery Plan" From the QTS White Paper Series

Rothstein Associates (2008), "Statistics and surveys-genera industry statistics", available at: www.rothstein.com/links/rothstein_recommended32.html (accessed 2 May 2008).

Rozek, P. and Groth, D. (2008), "Business continuity planning. It's a critical element of disaster preparedness. Can you afford to keep it off your radar?" Health Management Technology. Vol 29



Rudestam, K. E. & Newton, R. R. (1992) Surviving your dissertation (London, Sage).

Savage, M. (2002) "Business Continuity Planning" Journal: Work Study

Sayen Organisation (2008) "Understanding Disasters" Internship Series, Vol. 3 available at <http://www.sayen.org/Volume-III.pdf>

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

Singleton, R.A *et al.* (1993). "Approaches to social research" (2nd ed) Oxford University Press.

Smit, N. (2005) "Business Continuity Management – A Maturity Model" Master's Thesis Informatics and Economics

Smith, J. A., Flowers, P. & Larkin, M. (2009). "Interpretative Phenomenological Analysis: theory, method and research". UK: Sage Publishers.

Snoyer, R.S and Fischer, G.A (1993), "Managing Microcomputer Security", Business One, Irwin, Homewood, IL, p. 431.

Sommer, R. & Sommer, B. (2002). "A practical guide to behavioral research: tools and techniques" Oxford University Press, Incorporated, 2002

Swanson, M., Lynes, D., & Gallup, D. (2010), "Contingency Planning Guide for Federal Information Systems". Nist Special Publication 800 – 34 Rev 1.

United States General Accounting Office (1999), Year 2000 Computing Crisis: Business Continuity and Contingency Planning, available at: [www.gao.gov/special.pubs/ ai10119.pdf](http://www.gao.gov/special.pubs/ai10119.pdf) (accessed 23 October 2000).

Wan, S. (2009) "Service impact analysis using business continuity planning processes" Campus –Wide Information Systems

Willig, C. 2001. Introducing qualitative research in psychology: adventures in theory and method, Buckingham: Open University Press.

Wilson, B. (2000), "Business continuity planning: a necessity in the new e-commerce era", Disaster Recovery Journal, available at: www.drj.com/articles/fal00/1304-02.htm (accessed 21 October).

World Medical Association (WMA) (2010), WMA Statement on Medical Ethics in the Event of Disasters, available at: www.wma.net (accessed August 16, 2012).

Wyckoff, K (2007) "Tips on Qualitative and Quantitative Data Collection Methods".

Yin, Robert, K. (1994). "Case study research: Design and methods", 2nd ed. Thousand Oaks, CA: Sage.

Yin, R. K. (1984). "Case study research: Design and methods". Newbury Park, CA:

Yin, R.K (2003), "Case Study Research: Design and Methods", Sage Publications, Inc, 3rd edition

Zainab, A.N., Chong, C.Y. and Chaw, L.T. (2013), "Moving a repository of scholarly content to a cloud", Library Hi Tech, Vol. 31 Iss 2 pp. 201 - 215



APPENDICES:

Appendix 1: Questionnaire



UNIVERSITY of the
WESTERN CAPE

Research Questionnaire for Master's Degree in Information Management

Reasons and identifying Business Continuity Plan failure after a disaster event

Research conducted by Fadeel Sambo

By participating in this research you declare that all information provided is true and accurate and can be used for the purpose of this research. Due to the nature of the interview and questions this interview will be recorded and transcribed at a later stage.

May I proceed with this interview and do you agree to the above declaration Yes

Name of Company: _____

Name of respondent: _____

Contact Details: (w) _____

cell _____

Email: _____

Department: _____

Position held within the company: _____

Signature of Respondent: _____

1. Does the company have a written business continuity plan?
2. Where is the company's BCP kept and who has access to this document?
3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?
4. Does the DRP form part of the BCP or is it a separate plan altogether?
5. Does business continuity and disaster recovery readiness have support of top management in your organization? And if not why?
6. What happens if key personnel are not available during a disaster?
7. Has your organization identified which vendors may need access to your facility after a disaster?
8. How often is the BCP reviewed and updated?
9. How are business critical applications identified?
10. Who is responsible for identifying these applications?
11. Was your disaster covered by your plan, if no why?

12. Do you perform back-ups faithfully and include every server and hard disk?

13. How often do you perform a BCP test?

14. Do you have unscheduled BCP test? If tested, did you pass your test?

15. Does the company BCP highlight what are acceptable downtimes after specific disasters?

16. Do you feel that these times are attainable?

17. What was the impact of the disaster on business?



Appendix 2: Summary of Questionnaire

In the tables below the companies will be abbreviated as follow:

- Company A (A)
- Company B (B)
- Company C (C)
- Company D (D)

Summary per question:

Table 2: Question 1

Question 1. Does the company have a written business continuity plan?				
Answers	A	B	C	D
Yes	X	X	X	X

Summary for Table2:

Each company that were interviewed has a written BCP. This was a prerequisite to continue with the interview

Table 3: Question 2

Question 2. Where is the company's BCP kept and who has access to this document?				
Answers	A	B	C	D
Kept on share-point for the whole company to view	X	X	X	X
The complete IT department	X	X		
At the Disaster Recovery Site	X	X		
Key players				X
Senior managers				X

Summary for Table3:

Every company that was interviewed has a copy of their BCP on a Share-point portal, thereby allowing every employee to view and familiarize themselves with the BCP procedures. Some companies has there BCP document stored at their Disaster Recovery Site, so that policies and procedures can be followed during the disaster.

Table 4: Question 3

Question 3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?				
Answers	A	B	C	D
Yes	X	X		X
Lack of additional technical personnel.	X	X		X
Unlikely events such as floods, tornadoes and so on.	X			
Non critical business applications due to budget constraints.	X			
Power failures as company is on the same sub-station as parliament and the chances that parliament would experience a power failure is very slim	X			
Not sufficient business staff involve in the plan, mainly for testing	X	X		X
No			X	
Everything is covered			X	
Location for staff to operate from				X

Summary for Table4:

Majority of the companies that were interviewed had exclusions and the most common exclusions were

- The lack of additional technical personnel
- Not sufficient business personnel involved in the testing process

Table 5: Question 4

Question 4. Does the DRP form part of the BCP or is it a separate plan altogether?				
Answers	A	B	C	D
The DRP is part of the BCP	X		X	
The DRP consist within the BCP		X		
The BCP covers all the natural disasters			X	
The DRP within the BCP covers the technical aspects			X	X
Separate plans that makes up a BCP				X
DRP is covered by IT and Operations				X

BCP is enterprise wide				X
------------------------	--	--	--	---

Summary for Table5:

All of the companies that were interviewed have a DRP as part of their BCP. Even though some companies have separate individual plans it still formed part of the BCP as a whole.

Table 6: Question 5

Question 5. Does business continuity and disaster recovery readiness have support of top management in your organization, if no why?	A	B	C	D
Answers				
Yes	X	X	X	X
There is a committee that monitors all the BCP Tests	X			
There is a Business Continuity Management (BCM) team that looks after enterprise wide BCP			X	
Top management just approve the budget, but aren't really concern about BCP				X
Top management does not fully understand the importance of BCP	X			X

Summary for Table6:

All the companies that were interviewed has the support of top management within the organization, however for some of the companies that were interviewed, their top management don't fully understand the importance of a BCP.

Table 7: Question 6

Question 6. What happens if key personnel are not available during a disaster?	A	B	C	D
Answers				
Vendors are on standby to assist	X	X	X	
Support from vendors		X	X	
There is an agreement with third party vendors for technical support in the event of a disaster		X		

All key personnel has alternative numbers from a different service provider			X	
All critical services have standby and escalation procedures in place			X	
Nothing, there aren't any support from vendors				X
No support from any outsource companies				X
All applications are developed in house to meet business specific requirements therefore systems are unique to business				X

Summary for Table7:

Majority of the companies that were interviewed has vendors on standby to assist them on their applications in the event of a disaster. One company however has no support from vendors as all the applications are developed in-house.

Table 8: Question 7

Question 7. Have your organization identified which vendors may need access to your facility during a disaster?				
Answers	A	B	C	D
Yes only for specific vendors	X	X	X	X
Service Level Agreements (SLA) are in place with specific vendors			X	

Summary for Table8:

All the companies that were interviewed has identified and allowed for vendors to access their disaster facility. Some even went to the extent of getting an SLA in place with vendors.

Table 9: Question 8

Question 8. How often is the BCP reviewed and updated?				
Answers	A	B	C	D
Every 6 months	X		X	
Annually		X		
Real time replication, that allows all new applications to be included automatically		X	X	X
Some critical applications are reviewed quarterly			X	
No formal review				X
BCP and DRP are treated as live documents and are updated as and when new requirements are presented				X

Summary for Table9:

Majority of the companies that were interviewed has real time replication, thereby allowing that all new applications are implemented immediately. Some companies also review and update there BCP every 6 months.



Table 10: Question 9

Question 9. How are business critical applications identified?				
Answers	A	B	C	D
Through general consciences among IT and Business	X			
No specific Business Impact Analysis Tools	X			
By the use of a matrix		X	X	X
A Business Impact Analysis Tool is used to determine the impact of each application		X		
All business critical services and systems are rated as per criticality. (Mission critical, business critical, non-critical)			X	
Owners of the application are responsible for the server on which the application reside				X

Summary for Table10:

Most companies that were interviewed use a matrix to calculate and identify critical business applications.

Table 11: Question 10

Question 10. Who is responsible for identifying these applications?				
Answers	A	B	C	D
IT	X			
Business	X			
Each business unit will sign off on their own application		X	X	
Business owner			X	
BCM Team			X	
Manager of the department in which the application reside				X
Information and security team				X

Summary for Table 11:

Of the companies that were interviewed, business units, business owners, business continuity management team and departmental managers signs off or take responsibility for the applications.



Table 12: Question 11

Question 11. Was your disaster covered by your plan, if no why?				
Answers	A	B	C	D
No	X	X	X	X
Our company shares the same sub-station as parliament and the chances that parliament would experience a power failure is very slim.	X			
Overlooked	X	X		X
It was not foreseen due to information not being available as problem was intermittent			X	

Summary for Table 12:

None of the companies that were interviewed had their disaster covered in their plan and the reason was that they overlooked that aspect within the BCP.

Table 13: Question 12

Question 12. Do you perform back-ups faithfully and include every server and hard disk?				
Answers	A	B	C	D
No	X	X	X	X
Budget constraints due to the size of data that will be safe to disk. Disks are expensive	X			
Test servers	X	X	X	X
Non critical business applications	X	X		
All business critical servers are backed up on a daily basis	X	X	X	
Real time replication		X	X	X

Summary for Table 13:

Each company that was interviewed do not backup every hard disk and server. Test servers and non-critical business applications are not backed up, however critical business servers are backed up on a daily basis through real time replication.

Table 14: Question 13

Question 13. How often do you perform a BCP test? When tested, what were the results?				
Answers	A	B	C	D
Every 6 months	X	X	X	
No not all the time	X	X	X	
Once a year an ICT test is performed. This is a technical test to ensure that we are able to restore all servers.		X		
A user test is done once a year to ensure that all applications restored are fully operational		X		
Some applications are tested quarterly			X	X
Insufficient disk space on server			X	
Test are performed on a departmental basis				X

Summary for Table 14:

Of the companies that were interviewed, majority of them perform a BCP test every 6 months and do not always pass each BCP test.

Table 15: Question 14

Question 14. Do you have unscheduled BCP test? If tested, did you pass your test?				
Answers	A	B	C	D
No	X	X	X	
Too expensive	X			
Testers need to be arranged before the time.	X	X	X	
Company is not ready for it		X		
Yes would like to do unscheduled tests		X		
Yes when new changes takes effect				X

Summary for Table 15:

Majority of the companies that were interviewed do not perform unscheduled BCP test as testers needs to be arranged before the time.



Table 16: Question 15

Question 15. Does the company BCP highlight what are acceptable downtimes?				
Answers	A	B	C	D
Yes	X	X	X	X
Form part of the BIA		X		
Uptime is 99%			X	X

Summary for Table 16:

All the companies that were interviewed have acceptable downtimes documented within the BCP.

Table 17: Question 16

Question 16. Do you feel that these times are attainable?				
Answers	A	B	C	D
Yes	X	X	X	X

Time frames has been thoroughly tested and agreed upon			X	
Due to the nature of our business we need to be up all the time			X	X

Summary for Table17:

All the companies that were interviewed feels that the downtime is attainable, even though majority of them has 99.9% uptime.

Table 18: Question 17

Question 17. What was the impact of the disaster on business?				
Answers	A	B	C	D
SLA was missed with business	X	X		X
Retail outlet had to trade manually as databases resides at head office	X			
No stock updates were sent to and fro from retail outlet	X			
Only cash transactions	X			
Clients could not trade		X		
Financial impact		X		
Possibility of losing clients		X	X	X
Entire call centre was down			X	
Reputation was damaged				X

Summary for Table18:

Most of the companies that were interviewed missed Service Level Agreements with business and the possibility of losing clients due to their unforeseen disaster.