CHAPTER 4: DRP IN MCSB SYSTEM BERHAD

4.1 Overview of Company

MCSB was incorporated in Malaysia on December 9, 1980 and commenced business on April 1, 1981. Today, MCSB is well established and has proven its potential as one of the leading Information Technology companies in Malaysia by being listed on the Second Board of The Kuala Lumpur Stock Exchange (KLSE) on June 24, 1993.

The MCSB Group of Companies is principally involved in computer network systems integration, software development, software application, education and training, Internet Application and Network consultancy services and other value added services related to the Information Technology industry. The MCSB Group of Companies is currently present in Malaysia, Singapore, Hong Kong, Indonesia and China.

One of the main factors contributing to MCSB's rapid growth is its total commitment towards providing "solution-oriented" packages, defect-free and competitive products which enable the Company to provide uncompromised after-sales support and services to all its customers.

For the purpose of this thesis, the main concentration is the KL office. MCSB KL is the headquarters for MCSB. In KL, there are seven business units departments and five other operation departments. These departments are Internet Professional Services, Systems Supports, Call Centre, Software Support, Education Services, Oracle Support, Linux Support, Human Resource, Finance, Procurement, MIS and R&D. In MCSB KL also reside the main infrastructure, applications and data. Among the application would Customer Information Systems, Sales Systems, Email Servers, Human Resource Systems, Finance Systems, File servers, Call Centre Systems, Oracle Development and last but not least customers source codes.

4.2 Development of DRP in MCSB

4.2.1 Business Impact Assessment (BIA)

Before the BIA is conducted in MCSB, it started first with an awareness program to all the management staffs. It is a two hours programmes that informed them as to what DRP is and how important it is to an organisation these days. During the program too, they were explained as to the steps in developing the DRP. Through this awareness programme too, the support from the management on the development was obtained. Refer to Appendix C for a sample training slides.

The Business Impact Assessment (BIA) was planned to conduct to all the departments in MCSB KL, this would means twelve departments. Unfortunately, because of resources and time, the emphasise of this thesis is on the applications that are in the computer rooms, which include Customer Information Systems (CIS), Email servers, Oracle Development and file servers. In the server room too, there is PABX centre and other tools that is use by the Call Centre.

Using the assessment form, as in Appendix A, key managers are interview in each department to determine the degree of impact if there is an outage on the systems. During the assessment, the evaluations were focusing on time sensitive business processes, potential monetary and customer relations.

The selection of the owners was good, as all the owners are also the key managers for the department. The assessments were done quite easily as the owner realised the criticality of their servers.

No	Systems	Department/s	Financial	Customer	Legal	Image	Owner
1.	CIS	Call Centre	> 5000K	Catastrophic	Critical	Critical	FL Chan
2.	Email servers	MIS	50K	Moderate	Moderate	Moderate	Ather
3.	PABX	MIS	200K	Moderate	Moderate	Moderate	Ather
4.	Oracle Server	Oracle Support	1000K	Critical	Critical	Critical	Nadiah
5.	File servers	R&D	2000K	Critical	Critical	Critical	Fan

In general, the BIA was conducted successfully and the right estimation of the loss was easily identified, as they know how much loss of information they are accountable for each individual account. Nevertheless, the response time was very slow as they have critical projects that required their time.

No	Systems	Class	Criticality	Description
1.	CIS	Class 1	Mission Critical	Need to recover within 4 hours or less, due to business critical
2.	Email servers	Class 3	Important	Recovery of applications can be deferred until processing has been normalised
3.	PABX	Class 3	Important	Recovery of applications can be deferred until processing has been normalised
4.	Oracle Server	Class 2	Essential	Need to recover within 24 hours following an outage
5.	File servers	Class 2	Essential	Need to recover within 24 hours following an outage

4.2.2 Site Risk Assessment

The next step is the site risk assessment, physical review of the computer room is conducted to prepare for potential causes of outages as well as to correct any deficiencies. During the assessment, there are few deficiencies that need to be done. The physical site, the alarm, temperature control and the raised floor were done according to the specification but the servers were not arranged properly. This would be hazardous if fire or people accidentally kick the computer cables.

The Un-interruptable Power System (UPS) was tested. UPS units can instantaneously supply power for anywhere from several minutes to several hours. Fire extinguishers are place and certified. The smoke detectors are operational and are wired to the central alarm system. Sprinkler system, are checked and certified periodically as required by the local code.

4.2.3 Information Backup and Storage Process

For MCSB, there are two types of backup, one is for each individual application systems and another one is for the computer room as a whole. In this thesis will be given one example for the computer room as for each individual systems, owner will be having the copy of the DRP for their applications. The backing up of mission critical data is extremely important to the reliability and recoverability of the businesses.

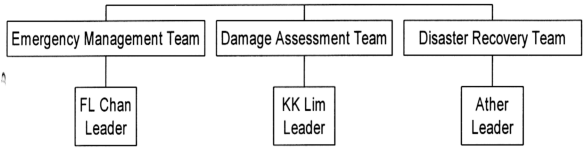
In beginning, a backup procedure was already in existence in MCSB. Unfortunately it was not updated accordingly and the format was not longer updated. Through this exercise too, the owners would be able to identified the important and less important processes in backup plan.

Because of the intensity and criticality of the backup process on the systems identified earlier, a jukebox was use to backed up data on a scheduled based. The frequency of the data being backed up would be depending on the owner.

All back-up data were stored with it's documentation in a secure location. Backed up data should be kept physically separated from the servers, with at least one full set of back-ups and associated documentation stored off site for disaster recovery purposes. The documentation and backup tape stored off-site must be only accessible to certain personnel only. The data and documentation were put off site data.

4.2.4 Recovery Teams

The next step of the process is to establish the recovery teams. The selection for member must be based on skills and authority. It is important to have a combination of the three teams to ensure the smooth process of recovery.



4.2.5 Critical Data

It is important and crucial to have information of critical data during recovery. During the process of determining the critical data was a problem as all the critical information was lost and misplace. Because of that, the MIS personnel had to recompile back all the information. This would include in all the vendors and suppliers handphone numbers.

The MIS personnel had to even look into the old invoices and finance data to find out information on particular software and hardware specifications. Network switches configuration and all the suppliers and vendors information on the specific products.

The directory of contact names is also. The directory listed out the emergency contact and numbers for emergency teams, networking contacts, critical users, contractors, vendors and also the local government.

4.2.6 Recovery Site

During the BIA, MCSB knows that they have critical application that need to be on within four hours. This is a Customer Information System that is used by the Call Centre to determine the customers calling in and delegating engineers to the customer's site. Since there is a need to charge the customers hence it is important to know the status of customers pre-paid unit balance.

A thorough plan has not been finalised on this matter at this point of time as there are few constraints involved and on top of that the limitation of resources that can fully focused on this DRP from Call Centre department.

For the initial stage, MCSB has agree to break the recovery site into two plans. The first plan would be to have the data backup and recovery would be at different building in KL, which the arrangement is currently being negotiated with the landlord and the next complete plan will be determine next year. The tentative plan would be to have the data replicated and backup in Penang. The feasibility study is yet to be start.

4.2.7 Assessment and Recovery Procedures

The next step to do is to develop the assessment and recovery procedures. The recovery procedure would be a step by step process as to what need to be done during the disaster.

The information was obtained from talking to the owner of the applications. This is part of the expectation of the application owners as to how they would want the recovery process to be. The procedure will include of how to detect disaster, how to declare a disaster and how to activate the recovery procedure.

4.2.8 Restoration Procedures

When the infrastructure and logistic of the recovery site is ready, the restoration procedure would take in progress. This is detailed out in the DRP plan.

4.2.9 Escalation Process

Escalation process needs to be established in MCSB. The Escalation Process is a procedure for operations and security people to follow in the event of a disaster.

4.2.10 Testing the Plan

In MCSB, DRP is not a new thing. It has been in the company for quite sometimes, until recently being paid attention closely after the September 11 attacked to US.

The DRP that was developed before, has not been tested at all and as the result when we first use them to recover some of the applications, it failed. Hence, the new DRP was tested and documented and stored properly.

It is important to test the recovery strategy and plan annually, based on the degree of business impact.

The testing need to be done regularly among the team. Keeping an updated plan is critical. The plan MUST be ready for execution condition.

4.3 Developing Standard Operating Procedures (SOP)

The next step in DRP is to have Standard Operating Procedures for the organisation. This is to ensure that if the next critical comes in the picture, the application owner would know what are the things that need to be complied when DRP are concerned.

In developing the SOP, it needed to be clarified clearly as to what are the scope of SOP that we are looking at. In the case of DRP, there are two main areas, one is the Information backup and recovery standard and the other are the disaster recovery plan. Both of them go together.

4.3.1 Information backup and recovery standards

The purpose of having the Information Backup/Recovery standards is for the protection of computer based information. The backup and safe storage of information is fundamental to the reliability and recoverability of each system and its supported businesses. In the event of information corruption or loss, disk hardware failure or site disaster, the backup information is often only link to recovery.

The owner of the computer applications, equipment and facilities in coordination with the application system owners are responsible to ensure the data is being backup.

These Information Backup/Recovery standards define requirements which must assist in providing for a timely recovery of critical business activities when an outage or a disaster occurs. In development of the SOP, areas of the possible failure need to be identified and replace with improvement by having certain standards.

4.3.1.1 Identifying Critical Information

The degree and scope of data recovery and backup planning is totally driven by the potential company and business impact that would result from the loss of a particular application, data, system, and/or network. An application's business criticality is based on several evaluation areas.

The methodology used to determine the criticality of business applications, data, systems, and/or networks is the Business Impact Assessment (BIA) process.

It is through this process that the business recovery requirements are defined. These requirements then provide the design objectives for the Information Backup Plan, recovery plan, as well as the recovery time frame by which the effectiveness of the disaster recovery process will be measured.

4.3.1.2 Backup Requirements for Critical Business Applications

Because of the need for rapid recovery, often with little or no loss of data (as defined by the Business Impact Assessment process), the backup methodology, frequency and off-site storage process used for essential business applications may vary widely.

A Business Impact Assessment (BIA) must be performed for each business application, system, and/or network in order to establish the true level of information criticality. The criticality classification and the backup process must be reviewed/updated by the application owner and equipment custodians:

The level of information criticality must be reviewed, documented and agreed upon by the affected application owners and equipment custodians.

An Information Backup Plan must contain the name of the system and or data, frequency and type of backup, offsite vaulting cycle and any trade off rational used in developing the backup plan.

4.3.1.3 Backup Requirements for Non-Critical Business Applications

Non-critical business applications and data must be fully backed up weekly. Incremental or differential backups must be done as required by the business.

All backup information must be stored with its documentation in a secure location.

Users of portable and/or remote systems are responsible for backing up and storing their data in a safe, secure location. The extent and frequency of the backup process is based on the business impact that would result from its loss.

4.3.1.4 Backup Procedures

Backup information provides protection from almost any threat - accidental or deliberate, that could cause loss or destruction of data.

A documented backup process must exist which defines the daily backup routines. At a minimum, it must include the following about the backup cycles: System Names or functional names included as part of any backup

Backup procedures must exist for handling daily backups as well as performing day to day restorations or full data recovery. The backup process must be automated wherever possible in order to ensure consistency.

4.3.1.5 Off-Site Storage

Off-site information storage is defined as a secure off-campus location that is sufficiently distant from the primary location so that, in the event of a localised or area wide disaster, the backed up information will be safe and available for recovery.

A documented procedure must be in place that outlines the off-site rotation process. A process must be in place for reviewing who has access to off-site processes.

4.3.2 Disaster Recovery Planning Standards

To state the Disaster Recovery Planning standards and responsibilities which are required for the protection of all business critical hardware, systems, applications and networks. Disaster Recovery Planning provides for the timely resumption of essential business hardware, systems, applications and networks in the event of a disaster.

Disaster Recovery Planning is a joint responsibility which is shared between "the custodians of the computer applications, equipment and facilities in coordination with the application system owners."

4.3.2.1 Identifying Critical Applications

The degree and scope of the Disaster Recovery Planning process is totally driven by the potential company and business impact that would result from the loss of a particular application, hardware, system, network and/or data. An application's business criticality is based on several evaluation areas.

The methodology used to determine the criticality of business applications, systems, networks and/or data is the Business Impact Assessment (BIA) process. The BIA process is the most important step in Disaster Recovery Planning. A Business Impact Assessment (BIA) must be performed for each business application, data, system and/or network in order to establish the true level of business and data criticality.

The recovery timeframe must be reviewed, agreed upon by the affected business and Information Systems areas and documented. Site-Risk Assessment must be performed to identify problems before they occur.

4.3.2.2 Developing a Disaster Recovery Plan

A Disaster Recovery Plan must contain all of the detailed steps, procedures and support information needed to recover the subject hardware, system, application and network in the event of a disaster. Because of the sensitive nature of the material contained in the recovery plan, it must be classified as Confidential Proprietary. A copy of the recovery plan, documentation and supplies must be kept in a secured off-site location.

4.3.2.3 Testing the Disaster Recovery Plan

It is impossible to overstate the importance and value received from testing the disaster recovery and back-up plan. Only through testing will any missing and/or critical pieces be identified that could have rendered the system UNRECOVERABLE.

System owners and equipment custodians are responsible for testing their Disaster Recovery Plans at least once a year to ensure that the plans are accurate, complete and that the off-site data can be used to successfully recover the application.

The test recovery must be successfully completed with the hardware, system, network, application programs, data recovered and the applications functionally verified by the business or application support areas within the recovery time frame that was defined in the Business Impact Assessment process. Failed tests must be re-tested, within a timeframe that is agreeable to the business area, until completed successfully.

4.3.2.4 Training

Training need to be provided for Disaster Recovery co-ordinators to ensure that they are aware of their responsibilities.