Volume 2, Issue 11, November 2012 ISSN: 2277 128X

www.ijarcsse.com

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Business Continuity Plans (BCP): An Introduction and Necessitate

Sudarshan Goswami[*]
Research Scholar, MU, Rajasthan
India

Dr. A. K. Vasishtha
HOD(AS), MTU, Noida
India

Dr. Sohan Garg
Director(MCA), MTU, Noida
India

Abstract— In the world of rapidly changing computer technologies and huge dependence on such technologies are increasing the risk of data loss. Unawareness and ignorance of environment is also leading the increase in risk associated with data storage systems. There are numerous conditions in which a financial institution or organization may face data loss leading to a huge business loss or dissatisfaction amongst the clients. Therefore it is must to have a Business Continuity Plan (BCP) effectively working in advance to protect the system from failure and also to restore from failure with minimum loss of data. In this paper we will introduce about the necessity of the BCP [9] followed by the reasons of critical data loses, challenges and responsibilities of different organizations and for this we will review the past work, finally the research papers will conclude about the future planning to reduce the losses incurred.

Keywords— BCP, RAID, MIS, BIA, DR, ORS, CRP, IS, IT

I. Introduction

Computer data may be one of your company’s most vulnerable assets and to have perfect, well maintained and periodically tested BCP is must for any organization. There are many situations in which data loss can occur but we will discuss few most important and recurring frequently here, that are follows:

(a) A RAID system’s collapses, causing its drives to overheat and fail.
(b) Some natural or manmade disaster happened leading to a system failure.
(c) A business adds a drive to its NetWare server, accidentally erasing the server’s partitions.
(d) An MIS administrator completes a fix on a mirrored drive without shutting off the mirror, losing the reference point for the original data.

A company attempts to restore lost data from carefully collected backups, only discovered that backups are unreadable. These disasters [10, 11] are becoming increasingly common. This is due to rapidly changing computer technologies. As drives get smaller and smaller, drive heads come closer and closer to the rotating media. The results are more frequent equipment failures and more destructive data losses. The increase in data disasters also stems from the sheer volume of data generated by modern companies and the decentralized way that data is produced, collected, and stored.

As distributed network models proliferate, and organizations continue to open their doors to the Internet, threats to data integrity and data security are compounded. While data backups would seem to offer an effective shield against these threats, backups do not always provide comprehensive data protection. That is because the data backup plans developed by many companies are not fully realized or, worse yet, not followed.

What is more, individuals often fail to test the “restore” capabilities of their backup media. If the backups are faulty, a simple data loss can quickly become a data disaster. Finally, even if backups are successful, they only contain data collected during the most recent backup session. As a result, a data loss can potentially take from you of your most current data, despite your backup attempts. The reality of data loss forces system administrators to ask themselves some serious questions.

1) Does a major data loss put your business interests at risk?
2) Does data loss expose your company to legal repercussions?
3) How susceptible are your data storage devices to corruptions and crashes?
4) What can be done to properly protect and recover critical data?
5) How often you have tested BCP.

The above mentioned questions raises issues for any organizations want to gain an edge over other organizations to provided services and support to their clients in time and in effective manner.

The importance of data to the daily transactional operations of any organization requires not only to raise these questions, but to successfully provide a solution as well.

This research paper will also help professionals and organizations to realize the importance and need to answer these important questions.

II. Critical Data Risks

According to an experience in the ONTRACK Data Recovery professional labs, the primary threats to organizational data and integrity collected from ORS (OnTrack Recovery Solutions) are as follows:

Cause of Data Loss	**Frequency of Occurrence**
Hardware or system malfunction	44%
Human error	32%
Viruses	7%
Software program malfunction	4%
Natural disaster	3%

In addition to being a vulnerable and a risky asset, computer data is also a valuable asset. According to a survey most businesses value 100 megabytes of data at $1 million. Using this figure as a starting point, it is easy to see how significant loss disaster the costs of lost or inaccessible data can be. The facts collected from CRP (Contingency Planning Research) are summary of an average hourly impact of lost or inaccessible data on a selection of different businesses are as follows:

TYPE OF BUSINESS	**AVERAGE HOURLY IMPACT (in Millions)**
Retail brokerage	$6.45
Credit card sales authorization	$2.60
Home shopping channels	$113,750
Catalog sales centers	$90,000
Airline reservation centers	$89,500
Cellular service activation	$41,000
Package shipping service	$28,250
Online network connection fees	$25,250
ATM service fees	$14,500

While the financial importance of data integrity is clear to most business executives, but the legal importance of data integrity is known to very few. According to [1] there exist a collection of legal precedents that can be used to hold a company accountable to those people affected by that company’s inability to cope with, or recover from, a disaster.

In other words, a data loss (temporary or permanent) could unnecessarily expose your company to customer lawsuits and other related legal actions. Coupled with its financial costs, the legal costs of a data loss could put your company’s future at severe risk.

Challenges and Responsibilities

Lost or inaccessible data can have a devastating, if not fatal, impact on your company. In fact, according to [2] the average company experiencing a computer outage lasting more than 10 days will never fully recover financially. Furthermore, 50% of these companies will be out of business within five years. The need to avert the business costs associated with data loss provides today’s IS executives with unique challenges and responsibilities. The primary challenges and responsibilities faced by IS (Information System) executives can be divided into three major categories.

1. IS executives must effectively manage mission-critical data that is distributed throughout a company on a wide variety of platforms.
2. They must deliver the same level of stability, reliability, and security provided by traditional, mainframe-centric operations.
3. They must support the data management requirements of all company users, including the need to assist those users who experience a data loss.

III. Review of Past Work

The benefits of integrating IT (Information Technology) into business operations are reportedly significant, the integration of operations into IS creates a serious liability. The primary risk is that the potential failure of IT infrastructure on which time-critical processes rely, can increase the likelihood that companies will go out of business when disaster strikes. Disasters can include business disruptions that result from terrorist attacks, power outages, security breaches, nature, and human error. Hayes [3] suggests that businesses create disaster recovery (DR) plans for IT systems that they determine are essential to operations. A DR plan "details the key activities required to reinstate IT services within agreed recovery objectives" after business operations have been interrupted by a disaster [4] Disasters interrupt operations for over 90 percent of businesses, nearly half of which close their doors within five years.

The purpose of this literature review is to describe key elements, supported by best practices, in disaster recovery planning for business information technology. The review is designed to aid IT professionals as they collaborate with business managers to determine (a) how each functional area depends on IT, (b) which IT systems are time-critical, and (c) how to recover those systems after a disaster.

The selected literature reveals that DR planning activities are divided into as few as three or as many as ten distinct categories.

This review organizes the major activities into five stages that are based on the models proposed by [5, 6, and 7]. These include Project Initiation, Conducting a Business Impact Analysis, Developing a DR Plan, Testing a DR Plan, and Maintaining a DR Plan have been discussed in the following table:

Table 1 – Five DR planning stages

Stage	DR Title	Process
1	Project Initiation	Businesses must establish the need for disaster planning and define a project plan to guide the development efforts (Clas, 2008, p. 47). An effective initiation process helps to assure the success of the resulting DR plan (Snedaker, 2007, p. 33). The major tasks included in the initiation stage are as follows: • Securing management support • Organizing the planning project team • Establishing the project management process • Obtaining the required resources • Developing initial project objectives
2	Conducting a Business Impact Analysis	A Business Impact Analysis (BIA) evaluates an organization's IT systems to determine which systems should be included in a DR plan (Gregory, 2008, p. 51), and in what order the selected systems should be recovered (Bradbury, 2008, p. 16). A BIA involves these tasks: • Gathering information • Identifying the time-critical IT systems • Performing a risk assessment • Prioritizing the recovery efforts
3	Developing a DR Plan	Based on the information revealed in the BIA process, this stage requires the identification and documentation of specific procedures to be invoked in the event of a disaster [6, 12]. The following tasks are required to develop an effective DR plan: • Selecting the risk management strategies • Defining disaster severity levels • Identifying activation triggers • Defining and documenting specific recovery processes • Selecting disaster response team members
4	Testing a DR Plan	Once a plan has been developed, it must be tested to ensure that it can accomplish the recovery objectives[8] that are defined in the BIA for each time-critical IT system. If problems are revealed in this stage, the DR plan must be revised and the test repeated [7]. Major testing tasks include: • Developing a test strategy • Training the recovery staff • Conducting the test procedures • Establishing the test frequency
5	Maintaining a DR Plan	During the maintenance stage, processes are established to guarantee that DR plans are reliably updated to reflect the current requirements of continuously changing business processes [2]. The tasks required to maintain a DR plan are as follows: •Identifying potential sources of change •Selecting the change management strategy •Maintaining the planning documentation

It is important to test the disaster recovery plan. Depending on an organization's culture and the preference of the response team leader, testing can be either spontaneous to simulate an actual crisis, or premeditated to encourage a "calm, rational" implementation of test procedures. Some organizations can chose to utilize both surprise and planned testing to give test participants experience with both approaches.

IV. Conclusion & Future Scope:

As We all know that Business data is very important and crucial, the loss may lead to entire business failures. The usage of Distributed systems and internet has added more risk to data spread all over the network. Once the data is lost, BCP helps a lot in recovering from the failure. This paper is of great importance to people professional or non-professionals to really think about a business continuity plans effectively working for their business data protection. It is must to have a BCP and also must to test the plan periodically.

References

[1] Tari Schreider, "The Legal Issues of Disaster Recovery Planning".

[2] Jon Toigo "Disaster Recovery Planning,"

[3] Hayes, J. (2005, October). Reaping the whirlwind [Electronic version]. IEE Review, 51(10), 29-29.

[4] Bradbury, C. (2008, April/May). Disaster! [Electronic version]. British Journal of Administrative Management, 62, 14-16.

[5] Spencer, R. H. & Johnston, R. P. (2003).Technology best practices. Hoboken: John Wiley & Sons, Inc.

[6] Snedaker, S. (2007). Business continuity & disaster recovery for IT professionals. Burlington: Syngress Publishing, Inc.

[7] Gregory, P. H. (2008). IT disaster recovery planning for dummies. Hoboken: Wiley Publishing, Inc.

[8] Rothstein, P. J., ed. (2007). Disaster recovery testing: Exercising your contingency plan. Brookfield: Rothstein Associates.

[9] Clas, E. (2008, September). Business continuity plans [Electronic version]. Professional Safety, 53(9), 45-48.

[10] Decker, A. (2005, January). Disaster recovery: What it means to be prepared [Electronic version]. DM Review, 15(1), 44-46.

[11] Gondek, R. (2002). Disaster Recovery: When more of the same isn't better [Electronic version]. Journal of Business Strategy, 23(4), 16-18.

[12] Toigo, J. W. (2002). Disaster recovery planning: Preparing for the unthinkable. Upper Saddle River: Prentice Hall PTR.