

Disaster Recovery and Business Continuity

Meshal Alabdulwahab

Abstract : Disaster recovery is a policy which is derived by an organization to help in the recovery or protection from a natural or man-made disasters. The disaster recovery tends to cater the IT infrastructure of an organization while the business continuity tends to cater all aspects of the business. Disaster recovery planning could help in saving a lot of money and energy of an organization. There are different sort of control measures which are needed to be taken by an organizations for disaster recovery i.e. Preventive measures, detective measures and corrective measures etc. A disaster recovery planner should undertake a number of strategies to prevent and control the damage from a disaster.

IJSER

Introduction

Disaster recovery could be described as a set of different policies and rules which tends to help in the recovery of technology based infrastructure which is affected by a natural disaster or a human created disaster (Berke, 2012). The main focus area of Disaster Recovery is IT and technology based system which are supporting different important functions of a business.

On the other hand Business continuity tends to analyze that how a business will operate after a disaster occurs (Aldrich, 2012). Disaster recovery is basically a subset of Business Continuity. Disaster recovery was first established in 1970 when the organizations tends to analyze their dependency on their IT infrastructures.

Classification of Disasters:

There are two basic types of Disasters:

- Natural Disasters

- Man-made Disasters

Natural Disaster could be of different types such as tornados, earthquakes, floods and hurricanes. It is very difficult to prevent from a natural disaster but good planning and different precautions can surely help (Schwab, 2013).

Talking about the Man-made disasters, it could be of different types such as IT bugs, material spill, failure of infrastructure, bio-terrorism etc. to counters such disasters proper surveillance, planning and testing is very important. These type of disasters could be reduced by precautions.

Disaster recovery planning:

Different researches have shown that Disaster recovery planning is a very good approach because it could help in minimizing the cost in long term (Lewis, 1999). So disaster recovery planning and

precautions could help in saving a lot of money for a company.

It could be said that now a day in any organization an IT system is very important, most of the organizations totally depend upon their IT infrastructure for daily operations. If the IT infrastructure goes down then surely it the daily operations of the company will stop or slow down, so it has become very important to analyze the importance of disaster recovery planning for example in case of a disaster some important data could be lost and might never recover (Sandhu, 2002).

Control Measures:

Control measures are the basic methods or steps which are taken by the organization to reduce the damage and eliminate different threats which could create disasters.

The disaster control plan is basically a subset of a larger program which is business

continuity planning, it includes the resumptions and recovery of following aspects:

- Data
- Application
- Hardware
- IT infrastructure
- Electronic communication

While on the other hand a business continuity plan includes the planning for different non-IT related items or aspects such as:

- Facilities
- Key personnel
- Reputation protection
- Crises communication
- Infrastructure

An organization could take different sort of control measures to eradicate or lessen the probability of loss from a disaster (Rubin, 2005). An IT based disaster recovery control

measures could be classified in to 3 basic types:

- Preventive measures

This sort of measures help in controlling and preventing an event from occurring.

- Detective measures

This sort of control measure helps in detecting any sort of unwanted event which could result in a disaster.

- Corrective measures

This sort of control measure helps in restoring the IT system after the occurrence of an event.

Strategies:

Before selecting any sort of a disaster recovery plan one must look in to the business continuity program which will eventually help in defining the main points about different businesses processes

(Toigo, 2002). A business continuity plan points out two metrics such as:

- Recovery point Objective

- Recovery time Objective

These metrics helps in sorting out different business processes which eventually helps in mapping the IT systems and Infrastructure. The defective RTO and RPO can easily defect a recovery plan (McEntire, 2014). Each and every item which is included in the disaster recovery plan requires a recover point if those recovery points are not generated properly then significant problems are created which are less significant to reduce the effects of a disaster. After mapping out the RTO and RPO according to IT infrastructure, the planner needs to identify a suitable recovery strategy. There are different strategies to protect data such as:

- Backup of data on regular basis could help in saving a lot of data.
- Replication of data could also help a lot in protecting the data.
- Now a day many cloud storage services are available which could be used to save the data as then data could be achieved from anywhere.
- Hybrid cloud system can also be used to save data.
- Antivirus programs can help in protecting data from any sort of virus or external attack.
- Fire extinguishers and alarms can also come in handy.

These strategies can certainly help in recovering and protecting the IT infrastructure from any sort of disaster.

Works Cited

Aldrich, D., 2012. *Building resilience: Social capital in post-disaster recovery*. s.l.:s.n.

Berke, P., 2012. Recovery after disaster: achieving sustainable development, mitigation and equity. *Disasters*.

Lewis, S., 1999. Disaster recovery planning. *Internal Auditor*.

McEntire, D., 2014. *Disaster response and recovery: strategies and tactics for resilience*. s.l.:s.n.

Rubin, C., 2005. Disaster recovery and hazard mitigation: Bridging the intergovernmental gap. *Public Administration Review*.

Sandhu, R., 2002. *Disaster recovery planning*. s.l.:s.n.

Schwab, J., 2013. Planning for post-disaster recovery and reconstruction. *Federal Emergency Management*.

Toigo, J., 2002. Disaster recovery planning: Preparing for the unthinkable.