Business continuity information technology

Technology, Information Technology

Introduction

In the present world, Disaster Recovery Procedures (DRP) is gaining greater attention. In today’s fast and rapidly changingenvironmentwith more reliance on InformationTechnology, the financial institutions are exposed to various risks in pursuit of their business objectives, the nature and complexity of which has changed rapidly over time.

In order to safeguard organization’s customers’ image and ensure continuity of its business needs to evolve and have in place a workable DRP for its IT infrastructure to minimize, if not control, the effects of risks. The type of threats/disasters, which can be encountered by the organization’s IT Infrastructure, disrupting the normal IT computing facilities, can be classified as under:

Short Term Threats/Disasters These are generally due to power, hardware and software failures, computer viruses, malicious hackers or simple operator errors. The results of these, which can cause temporary disruption to the computing operations, can be overcome in a short period. Extended Term Threats/Disasters happens may be due to disasters like strikes, fire and malfunctioning of IT hardware and allied facilities.

To over come from such disasters, some time may or may not be required, depending on the severity of damage done to the IT operational infrastructure. If these are for extended period of time, the backups should be place to over the disruption of computing facilities.

Sometimes we witness “ Total Disasters” This may be due to a fire, storm, earthquake or any other natural calamity, making IT infrastructure totally inoperable. If this situation is faced, functional backup site, together with the required IT Infrastructure should be in place to ensure availability of continuous IT computing facilities. Each of the above threats/disasters can have an adverse effect on the IT operations of the organization.

Depending on the severity of the threat/disaster, which can be for a short/extended period or total disaster, the IT computing facilities can become inoperative and can have serious impact on the business. To safe guard the continuity of IT computing facilities and overcome the threats of such situations, it is of vital importance that a Disaster Recovery planning is in place.

Backup Procedures are the primary objective of having backup procedures in place is to enable the organization to survive/recover and continue its normal business with full or partial IT operations, whenever the IT infrastructure is faced with threats/disasters. In order to overcome the effects of these threats/disasters, effective backup procedures have been put in place which will help in restoring the IT computing facilities to:

- Survive and resume normal banking operations which may be disrupted due to internal / external threats/disasters within a reasonable time frame.
- Avoid lost productivity and idle employees.
- Increase reputation for customer service.
- Gain customer confidence and goodwill.

Disaster Recovery Procedures (DRP)

For any short-term disruption of IT computing facilities, which may take place due tofailureof any software, the concerned IT Operations staff would take out the backup copy of the related software and load the same on the server for quick resumption of IT computing. For extended term malfunctioning of the hardware, the software once the backup hardware has been provided or repaired by the vendor, the IT Operations staff would load the software of the effected hardware to resume early IT computing.

In case of a total disaster situation of any IT computing facilities at any location/premises of Karachi, all backup software’s would be retrieved from the off site location where it has been stored by the IT Operations staff. The IT staff would make arrangements to load the same on the hardware of the pre-determined backup site for early resumption of IT computing.

In case any of the software in use is malfunctioning, the backup software would be loaded to overcome the problem. For short-term threats/disasters, the disruption of IT computing facilities due to malfunctioning of IT hardware and allied facilities would be for a short period of time (*Short term* is a relative term and is left to be decided by the concerned Business Head(s) for consequent restoration by the IT).

The situation arising would not lead to serious consequences as the temporary disruption would be normalized in a short p of time and thus no DRP is required. Malfunctioning of IT hardware and allied equipment, which would disrupt the computing facilities for an extended period, could have serious consequences on the banks business and IT operations. Locations where IT computing facilities could be affected by extended threats/disasters are as follows:

If malfunctioning of critical hardware or allied facilities at any of the above locations is experienced and evaluated to continue for an extended period of time.

In case of malfunctioning of E-mail server hardware at any of the above locations, the IT Staff would immediately contact the local or nearest office of the vendor and report the same. If the repair of the effected hardware is to take long, the concerned vendor will be asked to provide backup hardware as per our maintenance agreement with them.

For successful implementation of extended term DRP for the above locations, details of hardware and allied facilities which could be affected have been earmarked with the names of persons responsible for making available the effected computing facilities without disrupting the banks business and operations for long.

Total Disaster

In case of a total disaster situation of any of the above IT computing locations, concentrated and quick efforts would be made to switch over to the backup site. The concerned staff of the effected offices in close liaison with the IT Operations and concerned staff of IT Department to ensure that IT computing facilities are restored at the earliest. For this all the required software would be loaded on the configured hardware.

As per market, practicethe network links with WAN terminates at the main hub; various topologies are used for connecting the branches on WAN, which are:

Narrow Band Radio

Spread Spectrum Radio

DXX

DSL

OFDM

WLB

TDMA-VSAT

Frame Relay

If there is a break in IT networking link for a short period, the situation arising would not lead to serious consequences as the temporary disruption would be normalized in a short p of time and thus no DRP is required. In case of a total disaster of any IT location/premises, the networking link would not be affected.

However, if the networking link were broken, arrangements for moving the IT computing of the effected location would be carried out by the concerned staff of the location and IT department. All out efforts would be made to shift the staff and IT computing equipment to the nearest location/premises. If networking link is broken it will be restored in close liaison with the concerned networkingcommunicationprovider.

Reference

Peter Gregory and Philip Jan Rothstein (2007), *IT Disaster Recovery Planning For Dummies*

http://en. wikipedia. org/wiki/Business_continuity_planning

Martin Wieczorek, Uwe Naujoks, Robert Bartlett, 2002, *Business Continuity: It Risk Management for International Corporations*