DISASTER RECOVERY PLANNING WITH A FOCUS ON DATA BACKUP/RECOVERY

Judith J. Johnson

January 26, 2001

INTRODUCTION:

The purpose of this paper is to address the need to plan for reliable data backup and recovery within a disaster recovery plan.

DISASTER RECOVERY PLANNING:

Definition of a Disaster:
"An event that creates an inability on an organization's part to provide critical business functions for some predetermined period of time." [10]

Definition of a Disaster Recovery PLAN:
"The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster".[10]

Definition of Disaster Recovery:
"The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions". [10]

In planning for disaster recovery, characteristics of a disaster must be defined. "Currently there are over 35 different types of threats that can cause catastrophic business disruption, and new and more heinous threats are on the horizon." [4]

Potential threats are generally classified into four broad categories:

1- Accidental – loss of power, transportation accident, chemical contamination, toxic fumes, etc.;
2- Natural – floods, earthquakes, hurricanes, tornadoes, etc.;
3- Internal – sabotage, theft, (ex) employee violence, etc; and
4- Armed conflict – terrorism, civil unrest, etc.

Corporate disasters may include events from the categories above but analysis reveals that many do not fit these stereotypes. "By not recognizing these problems for what they are people often compound the problem through human error, poor decision making or poor planning". [3] As an example, in an IT environment, a programmer could update a production database without proper testing and without following an implementation process, which could result in the database becoming corrupt. This inattention to detail could bring down a production system causing a major business interruption. To compound the problem, if data backups were not being done or the backup schedule was inadequate, resumption of business would fail or be unnecessarily delayed.

An organization must analyze what needs to be achieved in order to carry on as though the disaster never happened. Information assets must be identified, such as data and source documents required for production database restoration, documentation required for restoring systems and data, and data that must be preserved to satisfy legal requirements and to reduce business loss. Therefore, a risk and business impact analysis must be performed to identify locations, functions, or applications most critical to your success. The organization can then determine how best to protect them.

DISASTER RECOVERY PLAN TESTING

"In order that your corporate issues are properly addressed, you must aggressively look for and address weaknesses in your contingency plan and frequently test your plan for failure to find the weakest links. A real disaster may not look like the test scenerios." [7] Many have been charged with meeting the requirement to put a disaster recovery plan in place - the mistake is not to test the plan and revise it periodically.

DATA BACKUP/RECOVERY PLAN:

Definition of Data Backup:

"Data backup is simply the backing up of data fields so that company personnel can go to the disaster backup site, restore files and application software, and be able to continue business as though nothing happened." [5]

It is critical that the method and schedule of data backups performed be sufficient to restore those processes deemed critical in the event of a disaster. "Backups are like insurance." [8] Listed below, as an example, are several options used to perform data backups within a Microsoft NT environment:

1- Full backup
2- Partial backup
   Incremental
   Differential
3- Disk imaging

OFFSITE STORAGE FOR DATA BACKUPS:

Off-site storage options must be considered. "Off-site storage is very arguably one of the most important components of an effective disaster recovery capability." [9] Data and source documents should be stored at a site separate from the location of the production systems. I have listed options for offsite storage below.

1- Cold site
2- Commercial cold site (leased facility)
3- Reciprocal backup agreement with another company
4- Service Bureaus (contracting for emergency processing services
5- Internet-based backup (subscribing to data backup/restoration through the internet)
6- Hot-sites (generic service bureaus equipped to run your applications)
7- Mobile recovery sites (delivery to the doorstep)
8- Redundant systems (in-house hot-sites over which the organization has complete control)

"It takes careful assessment and planning to identify the site that best matches both the company's needs and budget." [3]

EXAMPLES OF DATA BACKUP SOFTWARE OPTIONS:

Results of a recent SANS Institute survey determined that the following products were the most popular in an NT environment:

Veritas BackupExec

Computer Associates ARCServe programs

Legato's Networker for a combined NT/Unix network was also mentioned as being a good tool.

The organization for which I work may be moving to CommVault Systems' Galaxy Solution. It was chosen as an option mainly because it could restore Exchange Mail at the mailbox level. The following are identified by CommVault as the key features:

"Key Features:

- Online backup and recovery of the entire Information Store, Directory Store or Public Stores.
- Use of MSDN APIs for all backup and recovery operations.
- Browse and find of individual mailboxes, folders/subfolders with context-based search for individual messages to reduce administrative overhead associated with small scale restores.
- Automatic management of transaction logs; circular logging is turned off which decreases disk space requirements and eliminates disk management tasks, resulting in better performance and lower storage costs." [1]

DATA BACKUP STRATEGY:

"A backup strategy plan is key to avoiding data loss. Schroeder outlines the issues that the plan must address.

1- How often should the backups be done?
2- What is the backup medium (cartridge, disk)
3- When will the backups be done?
4- Will the backups be manual or automated?
5- How will it be verified that the backups occur without errors?
6- How long will backups be saved?
7- Where will the backups be saved?
8- How long will it take to restore the last backup?
9- Who is responsible for assuring that backups are done?
10- Who is responsible to do backups and restores if the primary person is not available?

These issues along with other issues that may be more specific to an environment must be addressed by the backup and recovery plan. Backup and recovery testing should address as many of the issues as possible attempting to find weaknesses in the strategy." [2] The data backup strategy ensures the integrity and availability of data needed for successful business resumption.

DIRECTION:

A group of hardware/software vendors led by Vixel Corp. have announced completion of a project that will enable IT managers to back up a SAN (storage area network) without sending the data over the LAN or through a server.

Advanced Digital Information Corp. began shipping a new Fiber Channel router that enables movement of data directly from disk drives to tape libraries across the SAN with limited Server intervention.

Organizations are now beginning to look into reducing traffic on their LANs and to free up more processing cycles on their servers by using serverless backups.

SUMMARY:

In planning for disaster recovery, we find that potential threats are identified specific to an organization and its critical business needs. Based on those assumptions, the organization must analyze what needs to be achieved in order to carry on as though the disaster never happened. A disaster recovery plan should be implemented, tested, and revised as necessary.

Including a well-defined data backup and recovery plan within the disaster recovery plan is a must. The integrity and availability of data are essential to a successful recovery of critical business functions.

REFERENCES:

1. CommVault Systems
   www.galaxy.commvault.com/products_sub.asp?Id=63

2. CSST Technologies,
   URL:www.cst-technologies.com/genericData_Backup_and_Restore_Testing.html

3. Hiatt, Charlotte, A Primer for Disaster Recovery Planning in an IT Environment, 2000, p.4,40,44

4. Hussong, Bill (1996). Corporate Executives:Have you Cared Enough?; Disaster Recovery Journal,*9(3), 44-48.

5. Lyons, Alan (1996). Effective Data Backup; Disaster Recovery Journal,*9(4), p.47-49.

6. McCright, John S. eWEEK, Vendors move to cut server out of data backup, (2000), URL:www.zdnet.com/eweek/stories/general/0,11011,2432158,00.html

7. Rothstein, Philip Jan (1996) Look Beyond the Disaster Stereotype; Infosecurity News, January/February, 49.

8. SANS GIAC Certification materials, NT Backups, (2000),p.4.

9. Tiogo, Jon William (1989) Disaster Recovery Planning:Managing Risk and Catastrophe in IS; Yourdon Press, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, p.77)

10. Disaster Recovery Journal, Glossary, URL:www.drj.com/glossary/glossary.htm