DISASTER RECOVERY PLANNING - WHAT? WHY? and HOW?

Bryan D. Clapper
HEWLETT PACKARD Company, Santa Clara, CALIFORNIA, USA

INTRODUCTION

Information is a major asset for all Corporations. More and more companies are relying on computers to store and manage this vast asset. In some industries, maintaining a competitive edge over competition requires this information to be on-line and readily accessible. This in turn, requires maximum system availability.

Data Center disasters can render this information inaccessible. Disasters can result from natural threats such as a fire, flood, or earthquake, to intentional acts by disgruntled employees such as theft or arson. But disasters don't have to be 6:00 o'clock headliners, they can result from operational mishaps or power outages or faulty equipment.

A disaster can cripple a company's access to accurate up-to-date information necessary for sound business decisions. In addition, disasters can hinder a company's ability to conduct normal business activities such as making/ receiving payments, meeting manufacturing schedules, booking orders, cutting purchase orders, and invoicing customers. Therefore, companies must be prepared to react quickly in the event of a disaster to minimize the impact to normal business operations.

Companies can achieve this protection by developing a **Disaster Recovery Plan (DRP).** Such a plan would ensure the continuation of normal business activity by restoring necessary data processing functions in a timely fashion. This paper focuses on **WHAT** a DRP is, **WHY** it is necessary, and **HOW** to develop one.

WHAT IS A DRP

A DRP is a comprehensive document containing the actions required to restore data processing activities in the most timely and effective manner. It is intended to reduce the confusion created as a result of the disaster by clearly defining a course of action. Below is a brief description of the sections contained in a Disaster Recovery Plan.

- Scope and Objectives
- Immediate actions/Disaster notification
- Reovery team - Roles and Responsibilities
- Accessing the Damage
- Recovery Procedures
- Application Requirements
- Checklists
- DRP Maintenance Procedure
- DRP Test Plan

SCOPE and OBJECTIVES

Will this plan ensure a "total" or "limited" return to normal data processing activities? The answer to this question will provide the SCOPE of the DRP. It will be determined by a clear understanding of what applications are critical to the company's success and how long the company can survive before data processing activities must be restored.

The objective of every DRP is to ensure the restoration of data processing activity in a timely and effective manner. "Timely" and "effective" are loose terms, however, that may need to be qualified. For example, the objective may be to restore ALL data processing activity in 24 hours with no major problems.

IMMEDIATE ACTIONS/DISASTER NOTIFICATION

Confusion can overcome individuals not trained on what to do in the event of a disaster. This confusion could compromise the safety of company personnel and/or result in unnecessary property loss. Thefore, it is extremely important to define and train all individuals on the immediate actions to take during a disaster. This would include procedures to ensure above all else, personal safety. In addition, it would offer procedures for shutting down the computer(s), securing the data center, notifying the proper authorities and contacting the Recovery Team.

RECOVERY TEAM - Roles and Responsibilities

This section would identify all of the individuals on the Disaster Recovery Team. These individuals would be divided into groups and given very specific responsibilities to execute during the recovery process.

Below is a chart proposing such groups and their associated responsibilities. The number and/or names of the groups is unimportant. What is important, however, are the FUNCTIONs they are responsible for performing.

GROUP	RESPONSIBILITY
1. Facilities	* Assess damage to the computer facility * Estimate the time to repair/reconstruct the facility * Manage the replacement and/or repair of the facility
2. Consumables	* Assess the damage to all consumeables (paper, forms, tapes, etc.) * Ensure timely replacement of required consumeables * Determine consumables requirements (specified in the DRP) * Recovery salvageable consumables
3. Operations	* Ensure successful operations at backup recovery site * Retrieve necessities from off-site storage (backups, documentation, etc.)
4. Software	* Assess software and application requirements for recovery

* Coordinate transfer of data and applications to the backup site
* Install all software (OPSYS and applications) at the recovery site

5. Hardware

* Estimate damage sustained by hardware
* Ensure the replacement and/or repair of hardware
* Recovery Salvageable hardware
* Coordinate transfer of useable and/or required hardware to backup site
* Install (user installable) hardware at recovery site

6. Communications

* Assess damage to datacomm equipment
* Ensure the repair/replacement of datacomm equipment
* Recover salvageable equipment
* Coordinate the transfer of useable and required equipment to backup site
* Establish network at backup site

7. Logistics

* Coordinate the transfer of hardware, software, consumables, data, and personnel to the backup site
* Provide transportation for all resources to and from backup site

ASSESSING THE DAMAGE

After a disaster has occurred, it is very important to assess the extent of damage sustained by the data center. This will be important in determining the appropriate recovery actions necessary to restore data processing activities. Based on the extent of damage, the recovery team will decide whether to continue processing on-site or relocate processing activities (all or part) to the backup site. Based on this decision, the appropriate recovery actions will be initiated.

RECOVERY PROCEDURES

This section will contain all procedures necessary to successfully restore data processing either on-site or at the backup site. In addition, it will identify what group(s) are responsible for the defined actions. Finally, this section will contain a procedure for returning from the backup facility. Below is a list of procedures to consider for this section.

* Notifying the backup site
* Identify applications to be recovered first
* Identify off-site storage retrieval requirements (consumables, documentation, data, software, etc.)
* Transporting resources to the backup site

- Configuration of the backup site
- Installing the operating system
- Installing the applications
- Scheduling applications/jobs
- Establishing datacomm links
- Instating security measures
- Restarting operations

APPLICATIONS REQUIREMENTS

This section defines and prioritizes those applications which are critical to the success of the company. Also, it defines all resources required by the applications including disc space, printers, paper, mag tape and datacomm equipment. Finally, it specifies the maximum amount of time the application can be "out of commission".

CHECKLISTS

Checklists are used as a reference guide by defining what resources are used and where they reside. For example, the consumables checklist would identify all consumables used in the data processing environment. In addition, it specifies the suppliers of these consumables, ordering lead time, availability and maybe even cost information. Listed below are the checklists maintained in this section.

- Consumables
- Off-Site Storage
- Hardware (CPU's, Memory, Terminals, Discs)
- Software (Operating system, utilities, applications)
- Datacomm Equipment (Modems, PBX's, Leased Lines)
- Documentation

DRP MAINTENANCE PROCEDURE

As companies grow, their data processing requirements and priorities change. These changes need to be reflected in the DRP as soon as possible. Therefore, a procedure for maintaining the DRP must be created and adhered to. DRP's that don't accurately reflect a company's business requirements are useless.

DRP TEST PLAN

DRP's, like software, must be tested for accuracy and effectiveness. Testing is designed to catch oversights which might prevent the Recovery from being successful. This section would contain such a test procedure.

WHY DEVELOP A DRP

Disaster Recovery Plans are required to recover from a disaster minimizing the impact to continued business. Justification for developing a DRP is found in understanding the costs associated with computer downtime. Some costs are quite easy to quantify while others are not.

For example, productivity losses in terms of salary for idle employees can be easily calculated. Assume, for instance, a company has an average of 60 on-line computer users per day and each user is active on the system an average of 5 hours/day. If the average salary for these employees is $10 dollars per hour and the computer were down for 1 day, salary costs would amount to $3000. If the system were down for one week that amount jumps to $15K and for a month $60K. Include in this model the cost for additional manual labor (manually tracking items through manufacturing, manually cutting invoices, manually writing checks for accounts payable etc.). Then add in the cost of interest expense for late payments to suppliers and the loss of valuable discounts for early payment. In addition, filter in the impact for delays of invoicing customers for products and/or services delivered. These delays in realizing income could greatly impact a company's cash flow position.

Intangible costs also need to be considered. Computer down time will directly affect the manufacturing and delivery of products. Delays in this area may destroy valuable relationships with customers and directly impact current and FUTURE business.

When the full impact of computer downtime is realized and costs are applied to the damages, the numbers can be staggering. It is then that the value of a disaster recovery plan is realized.

HOW TO DEVELOP A DRP

The development of a DRP requires the commitment of upper level management. This ensures that the appropriate (required) resources are available to develop, maintain, test and implement the DRP. The following steps are required in developing a DRP and are described below.

1. Assemble a Disaster Recovery Team
2. Define Company's business requirements
3. Define the DRP's scope and objectives
4. Develop the recovery plan.
   a. Identify critical applications
   b. Establish priorities for critical apps
   c. Define the resource requirements to run the applications
   d. Define the recovery alternatives (backup site)
   e. Develop damage assessment procedures
   f. Develop the recovery procedures for each alternative
5. Develop DRP maintenance plan
6. Develop DRP test plan

ASSEMBLING A DRP TEAM

The team should consist of representatives from Management, MIS, Facilities, and the various user communities. Including these groups in the development process adds viability to the plan. Management can relate business priorities and requirements which could directly affect the content of the plan. Users, for example, could bring information about their priorities, needs and concerns. In addition, these participants may be exposed to areas where their departments are vulnerable to disaster allowing corrective action to be taken beforehand.

DEFINING the COMPANY'S BUSINESS REQUIREMENTS

This step is necessary to determine what applications are most critical to the success of the company. Critical applications are those that directly impact cash flow. For instance, if an invoicing system is disabled, customer billing will be late and consequently payments for products and/or services will be late. This could adversely affect a company's cash flow position.

It is important to define for each application what costs (productivity, loss of business etc.) are incurred if down for 1 day, 1 week, or 1 month. This analysis will determine how long a company can survive without computer services.

DEFINING the SCOPE and OBJECTIVES of the DRP

Based on the company's business requirements, the SCOPE and OBJECTIVES of the DRP will need to be sufficient to ensure the company can operate (hopefully at a profit) in the event of a disaster. If it is determined, for instance, that the company must be fully operational (i.e. recover all applications) within 48 hours of a disaster, then the SCOPE of the DRP is to recover all applications and the objectives would be defined to meet the 48 hour requirements.

Once defined, the development team must review the scope and objectives with management and get approval to continue the development of the DRP.

DEVELOPING the RECOVERY PLAN

A tremendous amount of data needs to be gathered and analyzed in this step. For example, all critical applications need to be defined and prioritized. This includes disc space requirements, printing requirements, consumable requirements and datacomm requirements. Once the requirements are defined, a backup site to meet these requirements must be located. Some alternates to consider include mutual aid agreements, hot sites, cold sites and shells. Procedures must be developed to cover all pre and post recovery actions. And finally, a DRP maintenance and testing procedure needs to be developed.

MAINTAINING the PLAN

Again, the DRP is not a static document. This plan must be kept updated to reflect the changing business requirements and changes to the data processing environment. The minute new equipment is added to the data center, the DRP becomes outdated. Ample consideration needs to be given to HOW and WHO will maintain the DRP.

One way to ensure the accuracy of the plan is to make members of the Recovery team responsible for a particular portion of the plan. Meetings could be held quarterly to incorporate/discuss any changes to the plan.

TESTING the PLAN

Finally, the plan must be tested to ensure completeness and accuracy. Minimally, the plan should be tested on a yearly basis. Theoretically, however, once a change has been made the plan should be re-tested. This quite probably would prove to be too costly and time consuming. Therefore, criteria will need to be set which will determine when the plan should be tested.

BIOGRAPHY

Bryan Clapper has been with HEWLETT-PACKARD for 6 years. His first 4 years with HP was spent as a Software Development Engineer designing and developing Sales and Field Service applications. The last 2 years have been spent as a Commercial Systems Engineer supporting HP customers in the Santa Clara, California sales office.