

BUILDING A COMPLETE DISASTER RECOVERY PROGRAM

Gregory A. Morris and Norman Moyer

**Hewlett-Packard Company
100 Mayfield Avenue
Mountain View, California 94043**

ABSTRACT

As businesses come to rely more and more on their computing capabilities, the cost of downtime in the event of a computer disaster is becoming increasingly severe. Businesses face mounting pressure from external auditors and internal staff to prepare for the possibility of a computer disaster. With the help of outside consultants, companies are developing detailed disaster recovery contingency plans and then supporting these plans with backup computer hardware. Unfortunately, companies often cannot go to a single vendor that meets both their planning and hardware backup needs. And it is rare indeed for a vendor to take the additional step of offering a program to expedite recovery of a disaster site.

Focusing on the dilemma companies face in putting together a complete disaster recovery program, this paper reviews pivotal disaster recovery issues and considerations. HP Disaster Recovery Services are presented as one solution to the problem of implementing a complete disaster recovery program.

SITUATION ANALYSIS: THE NEED FOR DISASTER RECOVERY SERVICE

The importance of computers in business has grown dramatically since the days when organizations looked to computers simply to facilitate numerical computation. Today, computers are fundamental to every aspect of business, from financial management to order processing to manufacturing. In light of this increased reliance on computers, there naturally is increased concern that computer operations be able to continue under any circumstances. A complete disaster recovery program can significantly reduce the impact of a disaster on a company's normal operations.

There are several specific reasons that companies are investing in disaster recovery programs:

- o **Financial Impact.** Computer disasters are costly. Every day that the computers do not function can mean orders lost, orders not filled, or, at the very least, implementation of cumbersome manual procedures.
- o **Business Survival.** Losses can mount so rapidly that a company's only viable option is to discontinue business.
- o **Audit Requirements.** Auditors are demanding that computer-dependent entities have testable disaster recovery plans.
- o **Government Regulation.** Government organizations are being forced to develop disaster recovery programs. Recent legislation sponsored by Senator Alan Simpson (R-Wyoming) specifies initial guidelines for computer security for all federal agencies and subcontractors to the federal government. The legislation, which is expected to be the first of several bills involving data processing security, includes a discussion of disaster recovery planning and hardware backup. Increasing legislative pressure is motivating private industry as well.
- o **Management Liability.** The Foreign Corrupt Practices Act (1977) established that management can be held criminally liable for failure to protect resources critical to a company's operations. Thus, management of computer-dependent companies are legally responsible for establishing disaster recovery provisions.

Any computer-dependent company, in any industry, needs to understand the potential impact of a computer disaster and act to minimize the impact. However, the need for a disaster recovery program is most critical in a few specific industries.

The financial services industry -- banks, insurance companies, investment houses, etc. -- has an especially great need for disaster recovery protection. The industry is highly automated and encounters the strictest of audit requirements. Manufacturing companies need protection because computer-aided manufacturing can literally grind to a halt because of a disaster, resulting in the shut down of expensive manufacturing processes. Companies focused on distribution have completely automated shipment coordination, and risk losing valuable business if a computer disaster paralyzes this function. The health services and petro-chemical industries also are beginning to invest heavily in disaster recovery programs. In addition, many other companies rely on computers for billing, payroll, and other critical tasks.

A COMPLETE DISASTER RECOVERY PROGRAM

Recovery from a disaster is not complete until all normal computer operations have been restored at the disaster site or at a replacement computer facility. To enable this to happen, a complete disaster recovery program explores and defines the actions to be taken before, during, and after a disaster.

Disaster Recovery Planning. A disaster recovery program begins with a detailed contingency plan for interim processing and actual recovery of a disaster site. Decisive action based on advance planning is the first step toward minimizing the impact of a disaster.

The objective of a recovery plan is to enable a company to resume processing of critical computer applications as quickly as possible, and not necessarily to duplicate the normal operating environment. The plan documents emergency procedures for resumption of critical data processing functions and provides for longer-term recovery of non-critical computer operations.

There are three approaches to developing a disaster recovery plan. First, a company can write its own plan, using its own common sense and publicly available literature and information. Although this is a straightforward approach to planning, companies that do their own planning are not able to benefit from the expertise that specialists can provide. A professionally prepared recovery plan almost always is more thorough than a plan written by untrained personnel.

Second, a company can obtain assistance from a planning vendor, in order to write a thorough plan on its own. Some vendors offer training in disaster recovery planning and provide comprehensive planning methodologies designed specifically for a given computing environment. This planning alternative requires substantial time commitments from company personnel, but helps ensure that a company's planning process identifies and addresses all of its particular needs. Furthermore, because a company still retains responsibility for writing its plan, the company can readily modify or update the plan without additional assistance. Ongoing testing and maintenance of a recovery plan is the only way to ensure having a workable plan when it is needed.

Third, a company can hire professional planning consultants to write a plan. This alternative can be quite costly and forces a company to rely on a consultant to update the plan. However, having a consultant write a recovery plan may save

time and make company employees available for other tasks.

Hardware Backup. Hardware backup services provide backup computer hardware on which a company can continue its computer operations during a disaster. The process of documenting a disaster recovery plan typically identifies precisely what operations need to be backed up and what hardware is required to accomplish this.

There are several categories of hardware backup service. The most common service provides a stand-by hotsite -- a computer room with a computer system, peripherals, and telecommunications capabilities. Although some portion of a company's MIS staff may have to travel to reach the hotsite facility, having access to a full-scale computer facility gives a company one of its best hopes for duplicating normal operations.

Mobile backup is a popular alternative to the hotsite. Under a mobile backup scenario, a vendor sends a small computer room located in a trailer to a predetermined location. Since mobile backup must be offered on a small scale, this backup alternative generally works best for smaller operations and in countries where having to transport a mobile facility over long distances is not a major concern.

Companies with access to an alternative site that can serve as a computer facility during a disaster may prefer express delivery of loaned hardware. Under this option, the company contracts with a vendor for loaned hardware until replacement hardware is available. Express delivery is appropriate for customers who need a relatively small amount of equipment and minimal technical assistance.

Many companies write disaster recovery plans without assistance; many others seek to provide their own backup program. Some companies are so computer dependent that they have their own backup computer facility. Since the full cost of the facility is borne by one company, this alternative is practical only when a company has especially unique equipment requirements or when data security is a major issue.

The reciprocal agreement, whereby two companies agree to share their computer equipment in the event that one experiences a disaster, is a backup alternative that does not require the services of a commercial vendor. Reciprocals are advantageous because companies can minimize the cost of backup and still have access to a large-scale, fully operational computer facility. One drawback is that companies with reciprocal agreements historically have not

reserved sufficient capacity for their reciprocal partners. A related drawback is that testing of recovery procedures usually involves disruption of normal operations for two businesses.

Disaster Site Restoration. Once a disaster strikes, a company uses its disaster recovery plan not just to implement interim procedures, but also to restore the disaster site. Vendors are available to salvage equipment and clean disaster sites; however, a company's primary focus typically is on obtaining replacement hardware from the equipment manufacturer. The manufacturer can alleviate this conflict by taking a strong leadership role in the restoration effort.

THE SERVICE DILEMMA

To be complete, a disaster recovery program must consider recovery planning, hardware backup, and disaster site restoration. Preparing for these three aspects of disaster recovery is essential for full protection before, during, and after a computer disaster.

Today, companies are able to turn to a variety of specialists to build their recovery programs. These specialists typically focus on one aspect of disaster recovery -- planning, backup, or salvaging. They develop expertise in their area of focus that gives customers confidence in the services being provided. However, although computer users must invest in all areas of disaster recovery, there is no natural link between the services provided by multiple specialists.

A single vendor that offers planning, hardware backup, and disaster site restoration assistance enables a company to have an integrated recovery program and develop a well-defined partnership with a single recovery services vendor. This may not be of value to the company whose operations are relatively uncomplicated, easily understood, or easily supported during a disaster. For many organizations, though, no price can be placed on the added security that is guaranteed by the consistency of working with just one vendor.

The multi-vendor dilemma is understandable because the disaster recovery industry is young. Many vendors are small, regional players. Few standards have been established. Nevertheless, heightened management awareness of the industry and an ever-greater need for recovery services are certain to bring about standardization of services. The Hewlett-Packard Company is an example of a

company moving in this direction by this year becoming the most-recent major computer manufacturer to offer a complete array of recovery services.

HP DISASTER RECOVERY SERVICES

HP Disaster Recovery Services presently consist of two products. Although the products are available separately, together they provide a complete disaster recovery program.

HP Disaster Recovery Planning. HP Disaster Recovery Planning supplies the knowledge and tools necessary to develop, document, and maintain a disaster recovery plan for HP 3000 users. Based on a planning methodology customized for the HP 3000 environment, the service provides a structure for a company's recovery plan. A PC-based recovery plan template enables customers to write a plan that conforms to site-specific policies, practices, and conditions. To enhance the value of the planning tools HP provides, HP Disaster Recovery Planning includes two days of on-site instruction on HP's planning methodology. Recognizing the value of involving the customer in planning, HP also includes a project management guide to facilitate plan development.

The methodology covers identification of critical applications and alternate processing procedures, administrative procedures during a disaster, management of computer inventory during a disaster. Procedures for testing and maintaining a recovery plan assist auditors in determining the soundness of customers' recovery programs.

HP Backup. HP Backup provides access to an HP 3000 computer facility in the event of a system disaster. The customer travels to a facility dedicated to disaster recovery to run essential computer operations. The facility is equipped with HP 3000 systems and peripherals, an additional empty computer room for customer use, and telecommunications capabilities that HP tailors to meet individual needs. Customers receive six days a year at the recovery facility to rehearse and refine their recovery procedures.

As the equipment manufacturer, HP is in a unique position to offer technical support to HP Backup customers and provide disaster site restoration assistance. HP Backup personnel are on site and on call throughout the recovery process -- both at rehearsals and during actual disasters -- to help translate customers' recovery plans into action, answer operational questions, and facilitate access to special additional equipment. At the disaster site, HP works with the customer in all activities from performing a preliminary

inspection of the disaster site to expediting shipment of replacement hardware.

CONCLUSION

The disaster recovery industry is still in its infancy. As the industry matures, vendors are likely to consolidate their services, as the necessity of a total disaster recovery solution becomes clearer. The total recovery solution takes a company from planning of recovery procedures to backing up computer operations during a disaster to re-establishing normal operations. The total solution means total protection of a business. Given the growing importance of computers in day-to-day business operations, HP Disaster Recovery Services is one of the first of what probably will become a variety of disaster recovery programs from computer manufacturers.

Gregory A. Morris is presently Systems Support Product Manager for the Product Support Division at Hewlett-Packard in Mountain View, California. In this capacity he is responsible for the development and marketing of disaster recovery backup hardware products. Gregory joined HP in 1987 and holds a Bachelor of Arts degree in Economics at Princeton University and a Master of Business Administration degree from Stanford University.

Norman Moyer is presently a Product Manager for the Application Support Division at Hewlett-Packard in Mountain View, California. In this capacity he is responsible for the development and marketing of disaster recovery planning products. Norm joined HP in 1985 and holds a Bachelor of Science degree in Economics from the Wharton School, University of Pennsylvania.

