Disaster Recovery Planning for Homesteaders

Introduction

The term "homesteading" comes from the days of the pioneers that settled in the mid-west and western United States. That situation usually meant that you were far from your nearest neighbors and had to be self-supporting. Also, you had to plan for disasters of many kinds such as storms, attacks, medical emergencies, lack of food and other supplies, and equipment repairs. As an HP 3000 customer that continues to get cost effective and reliable use of your equipment for many years into the future, you must be self-sufficient and plan for modern day disasters to ensure a stable and protected environment.

This paper will not go into the details of writing a disaster recovery plan, but we will discuss the main points to consider. There are extensive resources available to tap for writing a plan such as doing a search of the Internet for the words "Disaster Recovery Plan" for companies offering solutions, papers presented over the years at the Interex HPWorld conferences and Solutions Symposiums, articles in the HP3000 Newswire, and various vendor sites like Robelle, HP Jazz, Beechglen, and Allegro. A request to the HP3000-L for sample plans and a search of its archives may produce results. The Disaster Recovery Journal at www.drj.com, Contingency Planning & Management at www.contingencyplanning.com, and Disaster Resource Guide at www.disaster-resource.com are some sites that offer a wealth of disaster recovery planning information. Paul Edwards & Associates offers a web-based product to produce a complete plan and provides a variety of consulting and training services.

Your HP 3000 system is probably the heart of your company's business operation. Some disasters, like disk drive failure, are minor, while others can destroy the computer center or entire corporate structures. The top ten types of disasters, which have caused the most damage in recent years, are power outage, storm damage, flood, hardware error/failure, bombing, hurricane, fire, software error, power surge/spike, and earthquake. Each of the various types of potential disasters listed has to be addressed in the contents of a recovery plan. The average time period in which essential company functions will continue, following a data center failure, is an average of 4.8 days for all types of industries. The loss of the data processing function and the most of the corporate records can put a company out of business. The current world situation requires that every company be prepared for almost any eventuality.

Systems Manager Notebook

Building an IS disaster recovery plan and the recovery of the data processing functions of the company is a vital part of the job description of the data processing manager. The earlier paper, "Homesteading: Plan for the Future", describes in detail the contents of the Systems Manager Notebook that is a starting point for constructing the IS plan. The contents of this notebook include hardware and software information that is vital to

recovering your system in any type of disaster. The rest of the company's business operating procedures has to be combined with the IS plan to form a comprehensive corporate disaster recovery contingency plan.

The Notebook contains hardware model and serial numbers, license agreements for all software and hardware, a copy of all current maintenance agreements, equipment warranty information, complete applications documentation of program logic, data file layouts, and system interaction along with system operator run books and any other appropriate documentation. There is a wealth of information contained in each HP3000 that can be printed and stored offsite that is critical to the recovery effort.

Vital output from MPE utilities and subsystems SYSINFO.PRVXL.TELESUP, SYSGEN.PUB.SYS, HPSWINFO.PUB.SYS, NMMGR.PUB.SYS, and DSTAT ALL list system configuration and status. Printouts of NPCONFIG.PUB and various NET.SYS files (SERVICES, PROTOCOL, HOSTS, INETDCNF, and RESLVCNF will provide networked printer and communications configurations.

SIU (Systems Inventory Utility) from the HP JAZZ web site and PSSWINVP.PRED.SYS will provide information about the various installed HP software subsystems. REPORT @.@ can help rebuild the accounting system configuration. BULDACCT.PUB.SYS creates two files, BULDJOB1 for MPE commands to rebuild the accounting system structure, capabilities, and access settings and BULDJOB2 for the MPE commands to rebuild the COMMAND.PUB.SYS file settings. Protect the access to BULDJOB1 because it contains all passwords! Backup $STDLIST from each full backup, which could be kept on tape, is useful to look up files that were backed up during each cycle. Use SHOWVAR HP@ system command to get system serial number, user limit, and other system settings.

Third party software installation codes are critical in case the system processor card has to be replaced or upgraded. You should have HP and third party vendor support phone numbers readily available. Hardware and software historical records along with MPE operating system and patch release history should always be recorded in the HP 3000 Gold Book that was delivered with each system. Terminal and PC configurations must be either printed for terminals or on disk for the PCs.

You should have additional copies offsite of the MPE/iX Software Maintenance Manual, MPE/iX release Communicators, and the Documentation CDs for all current manuals. These manuals are available from the www.docs.hp.com web site, also.

The Systems Manager Notebook is vital to the proper management of any HP 3000 site and is part of the Disaster Recovery Plan. Every site should have one because it contains critical hardcopy information to back up the information contained on the system. It is used to manually recreate your environment as a last resort. All parts of the notebook have to be kept current at all times and it would be prudent to store a copy off-site.

Disaster Plan Contents

A proper Disaster Recovery Plan is comprised of two major parts that are combined together to produce a proper plan. These are database elements and the written procedures to recover from each type of disaster. After inputting all the required data elements and customizing the recovery procedures, the planning tool you use should provide the capability to print the complete plan, or make it available in an electronic format for distribution to all appropriate corporate personnel. Your plan is a living document that has to be kept current at all times to be effective.

The database elements are equipment, facilities, forms, personnel, software, supplies, vendors, and vital business records. Equipment information includes manufacturer, serial number, model number, and warranty terms. The locations and communications capabilities of all physical facilities are required. All special forms and supplies used in the corporation should be identified along with vendor information required to procure additional stock. Contact numbers for all personnel involved in the recovery teams must be kept current. Locally produced software as well as third party vendor products must be identified along with any special codes required to allow the proper execution of the software on a recovery system. Vendors name, address, contact name, and phone number for all equipment, supplies, software, and recovery site are vital to the recovery process. The locations of any vital business records have to be available to the recovery team after the disaster to help restore the business continuity of the company.

The written procedures in the plan will detail all steps required to deal with each type of disaster, from disk failure to loss of the data processing facility. Most plan production tool vendors will supply a template of boilerplate documentation to recover from several types of disasters. You will have to customize the provided template to fit your own organization and requirements. These templates are usually in a popular word processing format, such as Microsoft Word. The proper repository for your completed plan is at a location that is not on your premises and is available for continual update as conditions and requirements change. This location should be Web based, if possible, so that you and the other recovery team members can access it even if access to your own facility is not available. Access to your plan information should be restricted by passwords and levels of access determined by you during the setup process.

Recovery Systems Options

There are several types of system agreements that can be utilized to get your business data processing operation functioning again. These are hot site, mobile system, cold site, and shared usage. The cost for each varies, as does the response time involved in being up and running.

With any of these recovery system options, the level of duplicating your current environment will depend on the capabilities of the third party vendor. Anytime you move your operation to another computer system, you have to make sure you have the appropriate run codes available from all of your software tools vendors so your

applications will run properly on the recovery system. By periodic testing of the recovery plan, you can determine any problems that may arise during a real disaster and refine your recovery plan accordingly. Remember, these agreements are similar to insurance. You assess the risks and costs involved and make a proper business decision that makes sense for your company.

Hot site systems are maintained for you at a third party location. These systems mostly duplicate the hardware you currently have installed at your present company office. Proper communications and sufficient user access is part of the service. Because these systems are available on a very short notice, the time to be functional is quite rapid. The cost is the highest for this option, but provides the best possible recovery. It is very easy to often do your recovery testing on these systems. Also, you may use the hot site for shadowing of your production system to shorten the recovery time considerably. This is the choice that is usually recommended, if you can afford it.

The mobile site system is a completely operational computer system in a self-contained trailer provided by a vendor that can be re-located to your company site or any other site you choose. It is a system on wheels that has built-in power and can easily be connected to outside communications. Since the system can be readily accessed, testing can be easily done when required. The cost is usually less than a hot site. How close the trailer is staged to your recovery site will determine the amount of time required to be operational. A concern would be condition of the access roads to your recovery location after a disaster.

A cold site is a pre-determined location. This location must be properly prepared for a quick installation of a system and the accompanying equipment with power, communications, and user access already available. This location could be another company building, but you have to hope that the location chosen is not in the disaster area. This option will cost less on an ongoing basis, but will take much longer to bring on-line. The computer equipment may be a system you have purchased and stored for this purpose. Or, you may have a contract with a third party vendor to have a system available on short notice to ship to your location. Proper testing of your recovery plan is very difficult or impossible in this case.

Shared access is the agreement between two companies to allow processing on the production system of one company in the case of a disaster at the other company location. This is usually the lowest cost option but there are many problems associated with this choice. Usually, companies have growth that doesn't keep up with the capacity of their system. So, the available storage space is probably limited and sufficient communications links for outside user access are usually not in place. There may not be all the third party software installed on the other system that is required to process your applications. It would be disruptive to the other company to do periodic recovery plan testing. This approach is not recommended.

Communications and Backup

In a disaster situation, the communications will be your responsibility and have to be planned for well in advance. During a wide spread disaster, most communications vendors will be so booked up with essential repairs that getting installation of equipment and lines will be impossible. So, plan accordingly. Communications can be designed to allow users to have access to the HP 3000 systems remotely with Virtual Private Networking either from remote locations or even from their homes.

Proper backup procedures are essential to preserving the data integrity of the HP 3000 systems and providing a means to recover the system without loss of critical information. Full backups should be done as often as weekly and partial backups produced daily. The creation of MPE Customized System Load Tapes (CSLT) should be done at least twice a month usually with the full backup. Offsite storage of all backup media at a proper facility that can provide the media on call is a must.

Installation of a RAID storage system will provide mirroring of all of your system and data file drives. A failed disk drive can be hot swapped without any down time required. This is an inexpensive and highly recommended addition to your installation.

A technology called shadowing or continuous data replication can be used in addition to media backup and will keep the system environment of the main site in synchronization with a remote hot site. This will facilitate the rapid switchover to the alternate system with a minimum of downtime.

As you continue to homestead, you have to periodically communicate with your HP 3000 third party software vendors to ensure that their licensed software continues to operate correctly, their support is still at the expected level, alternate means of changing any copy protection codes are available, and the company is responsive to your communications around the clock.

Summary

The US Congress approved the Accounting Reform Bill or Sarbanes-Oxley Act that was sponsored by Banking Committee Chairman Paul Sarbanes and House Committee on Financial Services Chairman Michael G. Oxley to tighten regulation of independent auditors and make company officers more accountable for their conduct. Aside from requiring corporate officers to take greater responsibility for the accuracy of financial reports, SOA mandates that organizations understand the risks that may impact the financial reporting process. A proper assessment of this risk environment would likely include lesser known operational and IT risks resulting from, among other things, inadequate disaster recovery or business continuity plans. Your company needs to have a complete plan in place now to comply with these directives and protect the business.

The most important part of a successful plan is the **periodic** testing and evaluation of the completed plan. This provides the opportunity to fine tune the steps and procedures of the plan and discover any gaps that exist. Periodically, use the data stored off site, continue to

train all levels of personnel, test the communications links, reevaluate the results, and modify the plan as necessary.

It is true that major disasters are rare. But, minor ones can happen at any time. It is also true that no amount of planning and preparation guarantees a successful recovery. However, a properly prepared and tested disaster recovery plan does increase the odds of a company surviving a disaster.