DISASTER PLANNING AND RECOVERY

by Dennis Heidner
Boeing Aerospace Company

ABSTRACT

This paper covers disaster planning and recovery. The author discusses traditional disaster planning methods and presents the idea of disaster levels. The author develops guidelines which can be used to perform risk analysis and write a comprehensive disaster and recovery plan. Finally the author discusses applicable tools which are available from the contributed library and third party vendors and ways these tools can aid your planning and software preparation.

INTRODUCTION TO DISASTER PLANNING AND RECOVERY

When the subject of a disaster plan is brought up, very often your co-workers react like you are crying wolf. "Why", they ask, "should we worry about the computer system when it has been running so well. Do not tempt fate by preparing for the worst!" Unfor- tunately, this is the old "head in the sand" idea. Any sane and intelligent data processing manager MUST pursue and develop a contingency plan for the loss of the computing facility; such plans are called DISASTER PLANS.

What is a disaster? Well, our friend Noah Webster says that a disaster is 'any happening that causes great harm or damage; serious or sudden misfortune; calamity'. The complete destruction of the computer facility could be no doubt called a sudden misfortune or calamity. By the same token could we not also call the temporary loss of the computer, at the end of the month when it is printing paychecks, a calamity?

When the word "disaster" is mentioned, almost always the first thought is that of an 'act of God' such as a flood, earthquake, volcano, tornado, hurricane, fire, etc. However disasters can also be the result of deliberate acts of vandalism, security breaches, critical application software failures, or even catastrophic hardware or software failure on the part of the computer or MPE! In addition the one element that we almost always forget is human error. Consider this situation: you have begun a WARMSTART after shutting the computer down so you can change the date and time. The portion of MPE called INIT has just started and for some reason the operator realizes that the wrong tape reels are on the drive so (s)he halts the computer. Unknowingly your operator has interrupted MPE at a critical point because the computer has already changed information in the volume labels. Now when the next WARM or COOLSTART is attempted, the computer will fail to boot!

DISASTER LEVELS: NOT ALL DISASTERS ARE CREATED EQUAL

How calamitous a disaster is depends entirely on the potential (or actual) loss that could be (is) incurred. It is possible to have a 'disaster' on a new computer installation before it is in production use such that the amount of loss is very insignificant.

What we want is some type of plan that will handle both the minor mishaps and the major disasters. The plan should be easy to follow, well thought out, and practiced! How do we develop such a plan?

It is here that I differ from the traditional concept of disaster planning. In the traditional method, plans are made only for the worst case loss. But remember the possibility of the 'worst case' occurring is actually quite small, whereas it is very likely during the life of your machine

that you will experience a 'minor mishap'. The first step is to determine the potential damage if you were to lose the computing facility for a short interval, a somewhat longer interval, and finally completely. Once you know the potential losses you can try to develop a plan that pays off for each case. Besides any 'major disaster plan' must draw on the techniques used to recover the application after minor mishaps. Why not, then, develop a plan which covers more then one level of disasters?

Designing a disaster plan for several crucial levels has distinct advantages: First, the plan for a major disaster must draw on the techniques used at all levels. Next it is a convenient way to document the stages at which you escalate the involvement of key personnel. In addition the marginal costs in the disaster plan are much more apparent. This allows better informed management decisions for the risk analysis and protection costs.

In many cases the multi-level disaster plan is simply a formally documented version of the currently used undocumented procedures that the data processing staff has already been using. At our site the disaster plan has three levels:

Level 1 The computer is down for up to four hours following an interruption. The time is spent recovering and verifying that the system/application is intact. During this time transactions are handled with paper and pencil. The work is then caught up over the next several days.

Level 2 The computer will be down for more than four hours but less than twenty-four. As part of the recovery procedure a special team is added to work a second shift entering the transactions that were collected on paper during the first shift. The following day exceptions are corrected by those who hand-wrote data the day before.

Level 3 The computer will be down for more than twenty-four hours. During this time transactions are made by hand. The special data entry recovery crew is standing by. The site team is actively considering the alternate site. If one is made available then the application is moved to the alternate site. Once installed the data base is checked for damages, and corrected. After the intial check out has been completed then the special data entry team is used to enter the accumulated paper work.

RISK ASSESSMENT

Risk assessment involves determining the cost of ANY form of system interruption.

Lost Opportunities

What is the value of the time lost when the computer is down? Opportunity costs are the value of opportunities foregone. If you are unable to sell an item because the computer is down then this would be an opportunity foregone. Other examples might include loss of sales because customers lose confidence in your ability to forecast future market trends properly and introduce new products.

Real Costs

While the computer is down, you will be experiencing costs that are directly related to the resource (computer) or the event. This becomes painfully apparent when the computer is no longer avail- able, and you have a number of data entry personnel idle. You will have employees who are paid and bored, a double whammy! The computer itself also has a cost associated with it. Remember that you are still paying for hardware and software maintenance; in addition, the computer (if it still exists) is depreciating.

Consider the temporary loss of the accounts receivable and mailing lists. This could cause a severe cash flow problem in many companies. If your data is used for manufacturing planning, the temporary loss of data may result in production slides and material shortages. This translates to lost sales!

Finally, what is the value of your data? This should be the most obvious, explicit cost; however, it is often forgotten. A simple rule of thumb is that the value of the data is worth at least the cost of the machine. Often it is worth much more than that.

GENERAL DISASTER PROTECTION TECHNIQUES

Backup Procedure and Frequency

The best protection against disasters is consistent and intelligent system backup procedures. That is to say, you should have an established regular backup procedure, performed by operators who know what they are doing, with a media that is reliable. The frequency and method of your backups, whether partial or full, should be worked out with your HP Customer Engineer and is dependent on your system activity.

A good complete set of backup tapes is the ONLY way to guarantee that you may migrate to another site if necessary.

Backup Costs

With backups being such an important protection, why not fully backup the computer everyday? The answer is simple: backups are expensive. These costs can be broken down into several categories: labor, computer down time, and materials.

At our site, we estimate the time needed to backup data on magnetic tape (HP7970) at thirtyfive seconds per megabyte of files. This figure includes the time that our operators must spend changing tapes, cleaning the drive, and labeling the tapes. Therefore, if our system contains four hundred megabytes of data, the time needed for backup would be 228 minutes, or almost four hours.

When a full backup is in progress, it is best if the computer can be made as idle as possible so that as many files can be backed up as possible. This requires that either the computer be made idle during the work day or that you have operators running second-shift backups. At some HP3000 sites, the computer is in use nearly 24 hours a day. Backup time is essentially the same as down time.

Roughly 30 megabytes of data can be stored on one 2400 foot tape (HP7970). This means that our four hundred megabyte store would require about 14 tapes. The current price per tape is in the 20- to 25-dollar range. We would expect tapes for one full backup to cost us about $300.

Finally, how long do you hold your backup tapes? We rotate our backup tapes every two months. If we were to backup the system every night, then we would need storage for more than 500 tapes! The material investment would probably exceed $10,000. We have not included in our rough costs the amount spent on the paper backup listing, drive wear and tear, or the fact that after a few months you finally bite the bullet and order a 6250 bpi drive!

Obviously it is usually not feasible to perform a full backup every night. HP recognized this and gave us the partial backup ability. However, if your application uses a large (e.g., 300 megabyte) data base and virtually all data sets are modified every day, then a partial is not much faster than a full backup!

Okay, so what's the final tally? Well, the backup costs will be roughly:

```
Backup$ = Cost of down time + materials + cost of partials in between

where:
    cost of down time = labor for recovery + idle labor + lost
                        use of computer

    materials         = cost of tapes + cost of paper
                        + storage costs

    cost of partials  = cost of partial down time
                         + materials + labor
```

Transaction Logging

Since it is unreasonable and, in some cases impossible, to have a backup for the computer every few minutes another technique must be used. Such a technique is called transaction logging. The basic concept is to make a copy of changes to databases. This separate change file then can be used with a known good copy of a database to resynchronize the data in the event of a system interruption. Transaction logging allows, in effect, a continuous backup of the database to be made. Unfortunately, only transactions made on IMAGE databases are automatically logged by HP software. There is third party software available which will allow you to log transactions on KSAM and MPE files also.

There is no such thing as a free lunch; logging does have costs associated with it. The additional overhead for systems with sufficient memory is a 3% to 8% reduction in throughput. With logging you must have a place for the transaction copies to go. If this place is a tape drive, then you have the added cost of the drive dedicated to logging. If you are logging to disc, then you must allow sufficient disc space or periodically shut down the application and switch the log file.

Alternate Site (Mutual Backup) Agreements

Locate computer installations with similiar capabilities which could act as a backup site. There are several varieties of backup sites. Richard Gray, in an article in the March/April 1983 Interact, described three common forms. They are cold, warm, and hot backup sites.

Cold Sites

A cold backup site is generally a computer facility all ready to be used except it is missing the computer. This type of facility has a limited usefulness. Any company using a cold backup site should have an agreement with the hardware vendor so that the downed site has a high priority on new equipment shipment when needed. The cold site agreement is attractive because of the low capital cost; again, the disadvantage is that in the event of a total computer loss, the down time may be days, weeks or months.

In evaluating the cold site approach be sure to include the cost of the empty shell (room). Typically user occupancy (UO) costs run $5 to $15 per square foot per year. This means that a empty computer room that is 15 by 20 feet, and has a UO cost of $10 per square foot, could cost $3000 a year.

Warm Sites

A warm backup site is generally another computer installation which will make room for your application. A typical warm site is a computer service bureau. A warm site has a low capital cost and potentially shorter response time than cold sites; however, there are disadvantages. You may have compe- tition for the computer if the disaster is not confined to your business. In addition, the cost of the service can be quite high.

If your company has more than one system (at different locations) it may be possible to establish warm sites within your company by adding additional hardware and software, so that the systems appear to be mirror images.

Hot Sites

A hot backup site is generally a computer which is idle, just waiting for a disaster to happen. This type of backup site provides the fastest possible method to get up and going again. The obvious disadvantage is the high capital cost.

Service Agreements

HP provides a wide variety of service contracts. It is important that you match the service agreement with your needs, not your pocketbook. If during your risk analysis you have determined that your maximum allowable down time is four hours, then you should have, at the very least, a four-hour response contract with HP! Do not let the cost of service contracts be the driving force if you really need fast response.

Some things to consider when considering service agreements: guaranteed up-time, hardware reliability, guaranteed response time, and, lastly, costs.

Site Protection

There is a lot of truth to the saying that "an ounce of protection is worth a pound of cure". Be sure to build fire protection into any computer facilities. If you are storing your backup media at the same site, look into the purchase of an UL-approved fireproof data safe. Remember also that in many cases the damage is not done by the fire itself, but by smoke or water. Fire extinguishers should be the HALON type only. In addition, keep a supply of fire-retardant plastic available. In a recent fire at the Department of Health and Social Services in the state of Washington, an alert disaster team was able to save the disc drives and databases from serious water damage by covering the computer system with sheets of fire-retardant plastic.

If your business resides in a flood plain, then you should place the computer on as high a floor as possible. Backup tapes should be kept off site, in a MUCH higher place. Finally, during the rainy season, it may be worth altering your backup cycle to cover the increased risk.

Is your computer room earthquake-proof? Although most disc drives would survive a moderate earthquake, we often add extra hazards by placing tall bookcases in the same room. Then, when an earthquake strikes, the case falls and destroys the drive. If you must have the book case in the same room, anchor it!

Recovery Costs

What does it cost to recover after a disaster? This simple question is not easily answered, since the recovery cost is a function of a number of variables. For instance, how bad was the damage? How long will it take you to assess the damage to the data base and associated files? When will the computer be available?

You will never be able to predict exactly the time and cost to recover, but you can learn to arrive at good "ball park" figures. This can only be accomplished after you have gained enough experience. The needed experience is obtained during the day-to-day operations and by running practice drills.

Getting It Right

All of us have experienced a condition known as system failure. The steps needed to recover after a failure and the time spent recovering are perhaps the most valuable piece of information when designing your disaster plan.

Disaster drills help fill the gap in the practical experience you have gained in your day to day computer operations. Remember, one of the simple corollaries to Murphy's law is: "If anything can go wrong, it will do so at the worst possible time." No disaster plan can anticipate all possible problems, but drills can help pin-point the obvious mistakes and omissions.

When you hold disaster drills, suprise as many people on the recovery team as possible. Try to make the drill as realistic as possible. Now that does not mean you have to have smoke coming out of the windows and the sprinklers going, but it does mean that if the drill is for a fire which has completely destroyed the facility, no one should go to his/her desk for notes, etc. Assign one person on the team to take notes on the events during the drill and what material was needed or missing. After the drill be sure to review the notes with all members of the team. Finally, if you found any mistakes in the plan BE SURE to update it!

Computer Insurance

Most insurance companies can provide insurance against loss of facilities or loss of data. Consider some form of insurance as a supplement to your disaster plan. But before signing on the dotted line, carefully check any insurance agreement for cost, the deductibles, insurance coverage, and, most importantly, exclusions!

The Balancing Act

By now you have determined the cost for each level of a disaster to your system. The trick is to devise protection schemes which will provide sufficient protection at less cost than the actual disaster.

THE PLAN

Remember, when a disaster does occur, your best system analyst may be on vacation in some inaccessible portion of the world. Therefore do not count on his knowledge! Instead, make sure that your disaster plan addresses what and which records are vital for your company, what steps may be taken to recover the data, salvage operations (if necessary), alternate equipment, and who will be doing the work! Here is a simple outline for a recovery plan for your site.

A) INTRODUCTION

B) DEFINITIONS

C) SCOPE OF THE PLAN

D) STATEMENT OF LOSS

1) OTHER SYSTEMS DEPENDENT
2) LEVELS OF DISASTER

E) ALTERNATE SITE REQUIREMENTS

1) GENERAL SITE INFO
2) CURRENT SITE LOCATION
3) RECOVERY TEAM
4) HAZARD PROCTECTION
5) SECURITY PROCTECTION
6) BACKUP PROCEDURES
7) CRITICAL DATA AND PROGRAMS
8) SPECIAL FORMS
9) HOURS NEEDED
10) DATA COMMUNICATION
11) MINIMUM HARDWARE
12) SPECIAL SOFTWARE
13) DOCUMENTION
14) TRAINING

F) RECOVERY TEAMS

1) LEVEL 1 RECOVERY CREW
2) LEVEL 2 RECOVERY CREW
3) LEVEL 3 RECOVERY CREW

H) RECOVERY PROCEDURE

1) RECOVERY TEAM MEETING LOCATION
2) LEVEL 1 PROCEDURE
3) LEVEL 2 PROCEDURE
4) LEVEL 3 PROCEDURE

I) POST-RECOVERY PROCEDURE

J) ALTERNATE SITE AGREEMENT

K) PLAN FOR UPDATING THE DISASTER PLAN

TOOLS MAKE IT EASIER

The following is a list of tools which are useful in planning and managing a disaster/recovery plan.

Backup & Sysdump Programs

Hewlett-Packard provides a backup procedure called SYSDUMP. Using the SYSDUMP facility you can perform either full backups or partial backups depending on how you answer the questions. If you wish to automate this backup process, then look into BACKUP and SYSDUMP from the contributed library.

BACKUP - Switches the system log file, then builds a stream job for the backup, and finally streams it.

SYSDUMP -Maintains the date of the last full backup and is useful in determining the frequency of partial versus full backups.

Account Structure Programs

An absolute necessity for any type of disaster plan is a current Accounting Structure list. Use this list to recreate the accounting structure after a NULL reload or to migrate your application to another computer. Several very intelligent users of the HP3000 quickly discovered that maintaining the Account Structure list manually was not only tiresome, often it was never done. Why not let the computer do the work? Well, here are several programs which do just that.

ACCSTRUC - This program creates a series of stream files which can be used to re-create the accounting structure from scratch.

ACCTGEN - This program creates a job file which can be used to restore all users, groups, and accounts to a null system.

BACCT - This program creates a job file which can be used to restore all users, groups, and accounts to a null system. In addition, it provides general reports on file access and user capabilities.

BULDACCT - This program creates a copy of the accounting structure.

DIRK - This is a general purpose directory-query program. DIRK extracts information about files, users, groups, and accounts by wild cards, and such items as file code, last access date, size, etc. One of the handy features of DIRK is its ablitiy to generate a stream job for a user account or the whole system.

UDC Utility Programs

Almost every HP3000 installation has customized the MPE commands with user definable commands (UDCs). These custom commands are often interspersed in critical stream jobs. For this reason it is important to keep a list of the UDC commands and files with any disaster plan. Here are some programs from the contributed library which will help out:

LISTUDC - This program will list the UDCs in effect for the system. The report generated is a handy reference to have in the event of a disaster recovery.

UDCLIST - This program generates a list which shows which UDCs are in effect.

CMDANAL - This program generates a list of UDCs which are in effect for the system.

Stream Job Utility Programs

It is entirely possible that the sole cause of a disaster on your system, is an unwanted visit by a computer HACKER. Currently the stream facility that HP has provided requires that passwords be inserted in the stream file. This poses a very severe security risk. If you must move to an alternate site, you do not want to be bothered with changing passwords on all of your files in addition to trying to recover lost data! Again the user community has come through and developed a number of very useful programs. These include:

DOJOB - DOJOB lets you build a job card template, then when a job is streamed, DOJOB looks up the necessary passwords and inserts them.

JES - JES allows you to maintain a schedule of when jobs are to run. JES supports job card templates and allows parameters to be inserted.

JOBQUE - JOBQUE lets you set up stream files to be submitted at any hour of any day. Other features include user notification if the job was not launched when requested (system was down, etc). In addition, JOBQUE supports a template which allows the users to build the stream jobs without including the passwords in their files.

SLEEPER - streams jobs, executes MPE commands, and runs programs at desired intervals.

SLS - An friendly interactive facility which streams jobs immediately, at desired times, and has job templates.

STREAMER - streams a job that passes system and site security and provides the passwords for the job cards.

MPE Data Recovery Utilities

The tools listed in this section should only be used by very experienced personnel.

SADUTIL - Stand alone diagnostic that allows file recovery. This utility is HP supported.

RECOVER2 - Restores files from the tape created by SADUTIL.

STAN - Reads the directory from the backup tapes and display the file creator information.

DISKED2 - Disk Edit utility program supported by HP.

Data Base Recovery Tools

HP provides four useful tools to protect your IMAGE data bases. These are DBSTORE, DBUNLOAD, DBLOAD, and DBRECOV. In addition, there are a number of tools available from third-party software firms, such as ADAGER from Adager, S.A., RECOVERY/3000 from Abacus, and SUPRTOOL from Robelle, to name a few.

STREAM JOBS MAKE EASY WORK

Simplify your disaster recovery procedures by establishing a couple of simple stream jobs. These jobs then can be used to recreate and restore the important files from your system on an alternate system, when necessary.

Stream Jobs For Accounting Structure

The following stream job uses the contributed library program 'DIRK' to create a file which can be used to recreate the complete accounting structure for your system.

```
!JOB ACCOUNT,<<USER.ACCT>>;OUTCLASS=,1
!COMMENT  ********************************************************
!COMMENT  *  This job creates a copy of the WIDGETS accounting*
!COMMENT  *  structure and places the output in a file called *
!COMMENT  *  WIDGETS.DATA   The file is used to recreate the  *
!COMMENT  *  the WIDGETS application at another site if the   *
!COMMENT  *  of a DISASTOR RECOVERY PLAN is invoked.          *
!COMMENT  *                                                   *
!COMMENT  *  This job is stream every night by JOBQUE.  The   *
!COMMENT  *  logon user is MANAGER.SYS.  We have a special    *
!COMMENT  *  file group call ACCOUNT.  When                   *
!COMMENT  *  we migrate to another site, we only need to add  *
!COMMENT  *  the ACCOUNT group to the host computer, and      *
!COMMENT  *  restore WIDGET1  into the group.  Then we stream *
!COMMENT  *  stream WIDGET1.ACCOUNT.SYS.  This will build our *
!COMMENT  *  needed accounting structure.                     *
!COMMENT  ********************************************************
!RUN DIRK.PUB.TECH
KILL WIDGET1.ACCOUNT
BUILD WIDGET1.ACCOUNT;REC=-72,,F,ASCII;DISC=3000,32,8
OUT WIDGET1.ACCOUNT
NEWA @;OKPASS
EXIT
```

```
!COMMENT   We are not worried about the file security for WIDGET1
!COMMENT    because we created the file group with CREATOR only
!COMMENT     file security rules!
!EOJ
```

We use the contributed library program JOBQUE to submit this job every night. This way a current copy of the accounting structure is always included with our partial and full backup tapes.

Stream Jobs for Reloading

The following job is an example of the accounting structure file which was created by the previous job.

```
!JOB NEWACCT,MANAGER.SYS;OUTCLASS=,1
!CONTINUE
!NEWACCT WIDGETS,MANAGER
!ALTACCT WIDGETS&
!STREAM ,#
#JOB NEW,MANAGER.WIDGETS,PUB;OUTCLASS=,1
#CONTINUE
#NEWGROUP PUB
#ALTGROUP PUB&
#;ACCESS=(R,X:ANY;A,W,L,S:AL;A,W,L,S:GU)
#
#CONTINUE
#NEWUSER MANAGER
#ALTUSER MANAGER;HOME=PUB&
#;CAP=AM,AL,GL,ND,SF,BA,IA,LG
#
#CONTINUE
#NEWUSER WIDGETS
#ALTUSER WIDGETS&
#;CAP=ND,SF,BA,IA,LG
#
#EOJ
!EOJ
```

To rebuild the accounting structure on a new host machine after a disaster, we simply restore the WIDGET1 file, and stream it. The passwords will be exactly the same as before the disaster. The next step is to restore the files from the WIDGET account, and begin our database recovery procedure.

Recovery

The exact recovery steps that you must follow depend on the type of disaster you experienced. In the case of the common system failure you can simply follow the standard procedures setup by HP. In the more complicated failure resulting in a disc crash, you may need to use some of the data recovery techniques discussed by Goertz and Beasley [1],[3].

Be sure to check your database for structural damage after any major disaster. It is also a wise policy to have a specialized program which checks the database for semantic errors.

After the Crisis

After the disaster is over, and you have successfully revived your application, it is time to review the steps taken during the crisis and incorporate any important new steps into your disaster plan.

Remember that you may have minor mistakes in your database for a number of weeks following any disaster. Make sure that your employees are aware of this fact, and that they report any glitches to the data processing department for investigation.

SUMMARY

In this paper we have discussed ways to place a value on the loss of your computing facility, the time to recover, and finally some of the tools that are available in the contributed library. As can be seen the developing a disaster and recovery plan is not a simple task. It requires careful thought and dedication on the part of your data processing department.

Appendix A is a check list of questions that can be used to determine if you have an adequate disaster plan. Appendix B is an example of a disaster plan for the ACME WIDGET company. Appendix C contains excerpts of the recovery plan for ACME.

Appendix A. Disaster and Recovery Check List

A) GENERAL PLANS

Do you have a disaster plan? Is a copy of the disaster recovery plan stored off site? Do you have a plan to update the disaster plan? Have you identified the disaster recovery team personnel? Have you identified an alternate meeting location? Is someone designated to keep track of the events during the recovery?

B) BACKUPS

Is the system backed up? What is the backup media? Do you periodically check your backup media? Do you maintain a list of files on the backups? Where is your backup stored? How long is your backup copy archived? What insures that a backup is done?

C) FACILITIES

How fire-sensitive and combustible is your computer room? Do you store unrelated materials in the computer room? Where is your excess paper stored? What type of smoke and fire detectors are installed in your computer room? Is there an emergency shutdown for the computer? Do you have a fire extinguisher and are your personnel trained to use it? Do you have fire retardant plastic which can be used to cover the computer and reduce water damage? Is the area under your false floor kept clear? What steps have been taken to protect the computer from brownouts and power surges? Is the building structurally sound? Can it withstand an earthquake? Are bookcases isolated so they will not damage the computer in the event of earthquakes? Are electrical junctions boxes under the false floor protected from water damage? What type of losses are covered by your insurance?

D) SECURITY

Is access to the computer room controlled? Is the computer room locked? How often is the lock changed? How many levels of LOGON passwords are required? Have you changed the passwords for the vendor-installed accounts? (Adager, Robelle, Quasar, etc.) How frequently do you change passwords? Do you monitor invalid logon attempts? How is access to your databases controlled? How do you handle security violations?

E) ALTERNATE SITE

Have you identified a possible alternate site? (cold, warm or hot?) Is the hardware and software compatible? Do you have a written agreement? Have you tested your recovery procedure on the alternate machine?

Appendix B. Sample Disaster Recovery Plan

1.0 INTRODUCTION

The WIDGETS application provides inventory visibility, on-line order processing, quality assurance (QA), materials requirement planning (MRP), marketing and finance information for the ACME WIDGET Company.

The WIDGETS application is critical to the conduct of ACME business. These procedures insure continued critical system operations and planned system recovery in the event of a local disaster.

2.0 DEFINITIONS

Disaster - a system interruption, local to the WIDGETS central processing system which does one or more of the following:

a. Disables the WIDGET system for more than 8 hours.

b. Permanently disables all computing hardware at the computer site.

c. Destroys critical data stored on tape or disk media at the computer site.

d. Disables system manager personnel at the computer site.

3.0 SCOPE OF DISASTER PLAN

This plan covers all applications and data which are used on the WIDGET1 computer. Excluded from the plan are the programming and new software projects which are being developed on the WIDGET2 computer. Peripheral support equipment (terminals) are excluded because we can satisfactorily meet our users' needs through priority reallocation of hardware and personnel.

4.0 WIDGETS IMPACT STATEMENT FOR LOSS OF SYSTEM

4.1 Other System Dependencies

The WIDGET1 computer does not pass any data to any other systems.

4.2 Stage 1

The WIDGET1 computer can be down for up to 24 hours with little or no impact on any external application. Down-time of up to 24 hours will require the system manager, ACME site manager, and a limited number of other personnel to be on hand to recover the programs and data base.

4.3 Stage 2

For down times of 24 hours to approximately 72 hours the WIDGETS data and programs can be recovered by providing additional manpower or overtime. We would expect to lose sales and a one week delay in shipment of our best selling WIDGET. Based on previous experiences, we can expect some minor complaints from customers, but no long term adverse effects on the company.

4.4 Stage 3

If the WIDGETS programs and data base are not available after 72 hours (3 days), the WIDGET recovery crew can no longer absorb the extra workload. At this point, there is a significant risk of loss of capital equipment, financial data, and MRP data. In addition, after 3 days it is probable that a number of our best customers would switch to the AAA Gadget Company. This loss of sales could have a significant impact on the future sales of spare parts, service, and maintenance.

5.0 WIDGETS BACK-UP REQUIREMENTS DATA

5.1 General Site Information

The WIDGETS system is comprised of an HP 3000 Series 30 computer facility and eleven remote peripheral support areas located throughout the greater Two Dot area.

5.1.1 Site Location

The WIDGETS site which is the subject of this disaster plan is located within ACME, Building 1, Room 2.

5.1.2 Widget System Contacts

ACME President - Honest Abe,
Work Phone 555-1234, Home Phone 800-1600

WIDGETS Operating Staff - Operations Manager, Jim Snodgrass
Work Phone 555-5693, Home Phone 556-8716

- Alternate, Paul S. Simon
Work Phone 555-3747, Home Phone 800-8263

- Manufacturing Manager, Issac S. Best
Work Phone 555-8732, Home Phone 556-4239

- Quality Assurance, Verl Y. Accurix
Work Phone 555-7777, Home Phone 556-9673

- Finance, Buck M. Green
Work Phone 555-8723, Home Phone 800-9623

- Clerical, Meg Good
Work Phone 555-9123, Home Phone 556-9673

5.1.3 Hazard Protection

Fire Protection - Conventional Overhead water Sprinkler System

Environment - Building Air Conditioning with Emergency Shut Down Switch

Electrical - Conventional Commercial Power with Emergency Shut Down Switch

Communications - Conventional voice grade telephone lines

5.1.4 Security System

Limited Access to Area - Simplex Lock

Logon Password - WIDGET System Access

5.1.5 Backup Frequency and Log Cycles

The WIDGETS application is fully backed up on Wednesday evenings. The backup tapes are maintained offsite (Building 2). In addition to weekly backups the WIDGET data base is stored, and a transaction log file is maintained. The log tapes are stored in the same room as the computer.

5.2 Critical Requirements, Applications, and Data

5.2.1 Application

The WIDGETS provides the following critical applications:

- Visibility on the location and use of a dynamic inventory of Widgets (4000 new widgets produced weekly).
- Random sample system for quality assurance.
- Market forecasting for sales
- Finance invoicing and payroll.
- Materials requirement planning.
- Production scheduling.

5.2.2 Interface

Critical interface with other systems include the following:

5.2.3 Programs, Data Bases, and Files

5.2.3.1 Critical Programs

All programs in the PROG group of the WIDGETS account are required for the application to run.

5.2.3.2 Critical MPE Files

All MPE files in the DATA, JOBS, REPORTS, and QUERY groups of the WIDGETS account are required for the applications to run.

5.2.3.3 Critical Vendor Software

The application programs require HP's MPEIV operating system with a version of Q-MIT or later. No third party vendor software is required.

5.3 Specific Forms

The type and quantity of paper required for proper WIDGETS operation are documented in the WIDGETS OPERATOR GUIDE.

5.4 System Usage and Hours of Operation

5.4.1 Normal Hours

The WIDGETS computer is used 24 hours a day by either on-line programs or background batch jobs.

5.4.2 Critical Hours

The WIDGETS computer must be available from 6:30 AM to 4:30 PM Monday through Friday.

If transaction logging is used, then the application and data bases need only be backed up on a weekly basis. Based on previous history the time needed to perform these backups is 4 hours once a week. If transaction logging is not used then this requirement is extended to 2 hours 5 days a week after 4:30 PM.

The WIDGETS application must have the computer exclusively the third weekend of every month for 20 hours. This time is used for billing and payroll.

5.5 Number of Ports Required

To continue operating, the WIDGETS programs require at least seven phone lines into the computer. There will be one phone line assigned to each of the following groups:

Manufacturing Quality Assurance Finance Order Processing WIDGETS data processing staff ACME WIDGETS president

The remaining phone line will be a floater; that is, anybody can logon to this port and use the computer for up to 15 minutes at a time.

5.6 Minimum Hardware Required for the WIDGET System is:

HP 3000 Model 30 or newer 300,000 sectors free disc space (75 megabytes) 7 1200-baud Bell 212A compatible phone lines 1 lineprinter 400 LPM minimum 1 tape drive for backups and logging. If the drive is not available for logging, another 50,000 sectors of disc space is required.

5.7 Documentation

See the WIDGETS operator and user manuals. After the WIDGETS system has been moved to the alternate site, extra copies of the user and operator manuals may be obtained by streaming USERGUID.DOCUMN and OPGUIDE.DOCUMNT.

5.8 Training

At least three of the recovery team members should have taken the system supervisor class from HP. In addition these members should also review the system supervisor material in the HP manuals at least once a month.

6.0 RECOVERY TEAMS

The recovery personnel fall into three categories: management, operating, and supportive. The management team will consist of the program manager, the ACME functional custodian, and the WIDGETS operation manager. The purpose of the management team is to assure that no unnecessary road blocks develop during the disaster recovery. The operating team will consist of the WIDGETS operation manager, the system manager, a representative from HP, and the WIDGETS analyst. The function of this team is to implement the recovery procedure as fast as possible. The final team is support personnel. The support team will consist of the remote site dependent staff and office personnel from the WIDGETS site.

7.0 RECOVERY PROCEDURE

The recovery procedure that will be followed is documented in the WIDGETS operators guide section 5.0 (Appendix C of this paper).

8.0 AFTER RECOVERY FOLLOW UP

After the recovery has been completed, stream the job called ERRCHECK.JOB to check the data base for structual damage and semantic correctness. The error checking job needs about ten hours to run to completion based on previous experience for the WIDGET system.

The section managers should also remind their employees that they can expect to find minor mistakes in the data. These errors should be reported to the WIDGET data processing staff on the appropiate forms so that they can be investigated and corrected.

If the disaster was a level 3, then all section managers create special teams to "inventory" their areas of responsibility. The WIDGETS data processing staff will assist in generating the needed audit reports.

Finally there will be a weekly meeting of the recovery team to discuss the status of the after-recovery inventories. The team will continue to meet and address any problems that arise until satisfied that the crisis is over.

After the crisis is over the WIDGETS operation manager will review the notes taken during the recovery procedure and make any necessary corrections in the disaster plan.

Appendix C. Excerpts from WIDGETS Disaster and Recovery Procedures

1.6 Emergency Shut Down

This section will cover two basic types of emergencies, a fire in the Computer Room and a disaster such

as Ash Fallout or similar incident that is predicted ahead of time.

1.6.1 Fire

In the event of a fire in the computer room there is a RED Emergency Disconnect Switch which is located just inside of the entry door on your LEFT. (It is just above the Line Printer). PULL the Center Section DOWN as the instructions on the switch direct. Then shut the door (make sure that it is UNLOCKED) and evacuate the premises. PLEASE BE SURE THAT YOU REALLY WANT TO USE THIS SWITCH. The only way that power can be restored to the room is by Facilities replacing the unit. IT IS NOT AN "OFF/ON" TYPE SWITCH.

1.6.2 Disaster

In the case of a disaster, such as an Ash Fallout, the following procedures should be used:

A - Get everyone off the system.

B - BACKUP the system. (See Chapters on System Backup, Data Base Store, and Weekly Backup Procedure.)

C - When the backup is done, shut the system down in accord- ance with the procedures in Paragraph 1.5.1 of this document.

D - Cover all equipment with the Fire Retardent Visquine which is located behind the door of the room. Please tape the Visquine to the bottom of all equipment cabinets.

E - Place all the tapes in the Tape Cabinet in plastic bags and replace in the cabinet. Be sure to shut all of the cabinet doors.

F - Secure the entry door to the Computer Room.

5.0 SYSTEM CRASH RECOVERY PROCEDURE

There are several different types of errors and levels of severity when CRASHES of the system and the data base are involved. If you are 100% sure that there were no data bases open*, then the data base recovery procedures listed below can be skipped. It would only be necessary to start a new log tape; however, if the FAILURE occurs when the system is active (users are on the system) it is a diff- erent story. *NOTE - When in doubt go through the full recovery procedure!

IN ANY CASE BE SURE THAT THE TAPE DRIVE IS FUNCTIONAL AND THAT THE TRANSACTION TAPES HAVE NOT BEEN CORRUPTED BY THE FAILURE.

The following section covers who to notify and how to determine the type of crash.

5.1. WHO TO CALL

Contact all users. Ask them to save all information on their last several transactions. Also get ANY INFORMATION displayed on their terminals (have them copy it EXACTLY as printed on the terminal). Tell them to shut down their terminals (logging off will not be necessary as the system has stopped). Inform the users that "WE" will notify them when they can get back on the system.

5.1.1 System Crashes Versus Transaction Logging Problems

5.1.1.1 Tape or Logging Failures

If the system has displayed a message which says that it is unable to write or use the transaction log, then the failure involves transaction logging only. The message will be similiar to the following:

ERROR WHILE WRITING TO USER LOGGING FILE LOGTAP (ULOGERR 7)

If such an error occurs then SKIP SECTIONS 5.2 THRU 5.6 AND

*** GO TO PARAGRAPH 5.6.5 ***

5.1.1.2 System Failures

In the event of a system crash that brings a halt to the HP 3000 (BE SURE THAT IT IS A HALT DUE TO A SYSTEM FAILURE), proceed with the following sequence of events.

Log the crash in the "GOLD" System Book and indicate any system failure messages that appeared on the console.

5.2 Memory Dump and Log Recovery

The MEMORY DUMP stores everything that was in the main memory of the computer to a designated device (Mag Tape or Floppy Disc). This data is later printed out on the line printer and used for analysis of the failure. Perform the dump in the following manner:

A. Rewind and remove the Log Tape from the Tape Drive, then mount a fresh magnetic tape and place the drive ON-LINE.

B. Press the "MEM DUMP" on the Front Panel, when the MEMORY DUMP aborts enter the following commands in from the console. You should have a ">" prompt.

>DUMPDEV 41,0 >DUMP

At this point the Software Dump Facility (SDF) will begin a serial execution of the file SDFCOM which is located on the system disc. Then the following message will appear on the console:

SOFTWARE DUMP FACILITY (VER XX.XX/XX)

When the HALT light comes on check and make sure that the tape drive is ON-LINE.

Press the RUN button on the front panel. The system will then dump everything that is in the memory to the tape drive and display:

DUMP COMMENT. IF YOU WISH TO CONTINUE WITH A WARMSTART COMMENT. THEN PRESS RUN. HALT

C. Press the RUN button on the front panel again. This will let the system begin the WARMSTART procedure. When the "RUN/HALT" field displays "RUN" hit the Return Key.

D. Reply to any questions that appear on the console (i.e., day/ month/year and time of day).

E. The system will issue a "Welcome" message and automatically logs on "OPERATOR.SYS;HIPRI". It will then print a series of lines of data depending upon the system configuration.

F. At this point IDLEJOB will ask if you want to proceed with the startup procedure. PLEASE ANSWER NO.

G. Remount the Transaction Log Tape and make any necessary replies to the console. Do a "SHOWLOGSTATUS". This should tell you that transaction logging is recovering. When the system indicates that logging has been recovered (or failed to recover), you may proceed.

H. If the system has indicated that Transaction Loging has recovered, use the console and do a "LOG WIDGTLOG,STOP".

FOR ADDITIONAL INFORMATION ON "MEMORY DUMPS" REFER TO THE SECTION ENTITLED "SOFTWARE DUMP FACILITY" IN THE HP 3000/33 OPERATORS MANUAL.

5.4 Saving the Transaction Log

In order to preserve the Log Tape for future analysis to determine if any data was lost, we want to put a copy of the Log Tape on the disc and get a listing from the line printer. This is done in the following manner:

A. From an Office terminal (if none were on when the system crashed you can logon by using ":HELLO ACME.WIDGETS;HIPRI") do a ":STREAM LOG.REPORT". This stream job transfers the log information to a disc and also lists limited information on the line printer.

   BE SURE TO EXAMINE THE LISTING! ESPECIALLY LOOK FOR THE FOLLOWING MESSAGE:

   BAD LOGID# nnnn TRANSACTION LOG IS SUSPECT!

   Then ..... please ..... DO NOT USE THIS LOG FOR A DATA BASE RECOVERY!

B. When the listing comes off of the line printer remove the Transaction Log Tape from the tape drive and proceed with the next step.

5.5 Rebuilding the Database

When there are several different databases in use at the time of a system crash, each database must be rebuilt independently. As we are currently using only the WIDGET database it is the example that we will use. The following procedures will bring your data- base up to date with the latest Data Base Store in the Tape Library.

A. From an office terminal enter ":DBUTIL" (or :RUN DBUTIL.PUB.SYS), the terminal will display the prompt: >>enter PURGE WIDGET When the system has finished your office terminal will display the following: Data Base WIDGET has been Purged >>enter "EXIT"

B. Mount the latest DBSTORE Tape on the tape drive. Place it on-line (NO WRITE RING PLEASE) and proceed.

C. From the office Terminal

   :RUN DBRESTOR.PUB.SYS

   The terminal will respond with WHICH DATA BASE? WIDGET

   Go back to the console and make your reply (REPLY (PIN#), 7)

   When the database has been restored the terminal will display "DATA BASE RESTORED" (this will take approximately one minute for each megabyte of database or about 40 minutes for WIDGET), and then display: DATA BASE RESTORED

D. When the restore is done remove that tape (hang it up with the other tapes). Then remount the log tape that was running when the crash occurred (NO WRITE RING PLEASE) and put the tape drive on line.

5.6 Recovering the Database

When the restore is completed you must RECOVER the database by using the Transaction Log Tape to the point it was as of the system failure using the following procedures.

A. From your Office terminal enter ":DBUTIL" (or :RUN DBUTIL.PUB.SYS), the terminal will display the prompt ">>".

```
>> enter ENABLE WIDGET FOR RECOVERY
     RECOVERY IS ENABLED.
>>DISABLE WIDGET FOR ACCESS
     ACCESS IS DISABLED.
>>ENABLE WIDGET FOR LOGGING
     LOGGING IS ENABLED. (it may show "Data base already
     ENABLED for LOGGING")
>>SET WIDGET LOGID=WIDGTLOG
     PASSWORD:  (USE THE RETURN KEY)
     LOGID:  WIDGTLOG IS VALID
             PASSWORD IS CORRECT
>>EXIT
```

B. From your Office terminal enter ":RUN DBRECOV.PUB.SYS"
the terminal will display the prompt ">".
>enter RECOVER WIDGET
DATABASE WIDGET LAST DBSTORED XXXXXX (The system will give the day, date and time - it is called a "time stamp"). If this is not the same as the date of the DBSTORE tape - ABORT the job.
>enter RUN

5.7 Storing the New Data Base

Now that the data base has been brought up to the same config- uration that it was when the system failure occured, we should make a new DBSTORE tape for protection. Mount a scratch tape on the tape drive and put it "On-Line"

A. From your office terminal do the following: :RUN DBSTORE.PUB.SYS (You may use DBSTORE alone) WHICH DATA BASE? enter WIDGET Then go back to the console and make the appropriate reply. When the DBSTORE is completed (approximately 20 minutes) your terminal will inform you that the job is complete. Remove the tape from the tape drive, take the write ring out, and hang the tape up in the tape cabinet.

B. After the DBSTORE you should shut the system down, then bring it back up with a "COOLSTART". This time when the system console asks if you want to proceed with "Start Up" procedures answer "YES". This is the only way to get IDLEUTIL running again. (Remember, when we started it up before we didn't start IDLEJOB.)

5.8 Start Transaction Logging

Mount a new tape (small reel please) on the tape drive and put it on line. From the Console do the following:

:LOG WIDGTLOG,START
/VOLUME ID FOR TAPE (MAX CHARS = 6)?
REPLY (PIN#),LOGTAP
/MOUNT TAPE VOLUME LOGTAP (MAX CHARS = 2)?
REPLY (PIN#), 7

The system will respond by saying that transaction logging is running.

A. Before proceeding any further you should allocate the programs as outlined in Paragraph 5.9.

B. Go back to the Console and do an "ALLOWLOGON".

This will set all the fences at the proper position; however, do ":SHOWOUT". If the out-fence is above 5 do -

:OUTFENCE 1

5.9 SYSTEM IS UP

Call the users and tell them they can log on to the system. Get a cup of coffee and relax - the panic is over, and the job is done. Please note, I may have left some of the responses from the system out of this writeup; however, all of your inputs and required replies are shown. Any system responses not shown are basically insig-nificant unless you get an error message, THEN CALL FOR HELP.

Bibliography

[1] Beasley, David, "HP3000 Data Recovery", Proceedings 1983 International Meeting HP3000 IUG, Montreal, Quebec, Canada April 24-29

[2] Gaade, R.P.R., "Picking Up the Pieces", Datamation, January 1980

[3] Goertz, Jason, "System Disaster Recovery: Tips and Techniques", Proceedings 1982 International Meeting HP3000 IUG, San Antonio, Texas, February 28 - March 5

[4] Gray, Richard, "Disaster-Recovery Strategies: A Back Door", Interact, March/April 1983

[5] Green, Robert M, and Heidner, Dennis, "Transaction Logging Tips", Proceedings 1983 International Meeting HP3000 IUG, Montreal, Quebec, Canada, April 24 - 29

[6] Heidner, Dennis. "Transaction Logging and its Uses", Proceedings 1982 International Meeting HP3000 IUG, San Antonio, Texas, February 28 - March 5

[7] Lazar, C.W., "HP 3000 Security/Risk Management", Proceedings 1981 International Meeting HP3000 IUG, Berlin, Germany, October 5-9

[8] Lloyd, Ben, "At the Movies", Interact, October 1983

[9] Lloyd, Ben, "Sane System Maintenance", Interact, September 1983

[10] Lohman, Guy and Muckstadt, John, "Optimal Policy for Batch Operations: Backup, Checkpointing, Reorganization and Updating", ACM Transactions on DataBase Systems, Vol. 2 No. 3, September 1977, pages 209-222

[11] Sardinas, Joseph, Burch, John G., and Asebrook, Richard, "EDP AUDITING: A PRIMER", Copyright 1981, John Wiley & Sons

[12] Sayani, Hasan, "Restart and Recovery in a Transaction-Oriented Information Processing System", ACM Workshop on Data Description Access and Control, May 1974

[13] Wise, Gerald, "Utopia", Hewlett-Packard Bonneville Regional Users Group Newsletter, February/April 1982

Dennis L. Heidner received the BSEE degree from Montana State University, Bozeman, Montana. He joined the Boeing Aerospace Company (BAC) in 1978 on a special project to review current techniques for management of general-purpose electronic test equipment. Based in part on this review of management methods used throughout industry, the BAC Test Equipment Management group received approval to buy a Hewlett-Packard HP3000 computer. Mr. Heidner was responsible for the system requirements planning, design and program implementation. In May 1980, the Test Equipment Inventory Management System became functional. Mr. Heidner has written "Transaction Logging and Its Uses", presented at the 1982 HP IUG in San Antonio, Texas. He was the co-author of two papers, "Transaction Logging Tips" and "IMAGE/3000 Performance Planning and Testing", which were presented at the 1983 HP IUG meeting in Montreal, Quebec, Canada. Mr. Heidner is a member of the IEEE Computer Society and the Association for Computing Machinery.
