# COMPONENTS OF A SUCCESSFUL LAN DISASTER RECOVERY PLAN

*By Leo A. Wrobel*

---

Technologists often exhibit an unexpected response when asked by management to produce a disaster recovery plan for an automated system. They get genuinely ticked off.

In the mind of a good technologist, this request is often interpreted as a signal that management does not trust them to recover in the event of a disaster. They look at the disaster recovery plan as some kind of a test to prove they know how to do their jobs!

Those responsible for technical systems in virtually any organization are capable of recovering from a disaster under virtually any type of circumstance. This may sound like a very surprising statement, especially coming from someone who writes disaster recovery plans for a living; it is however, quite true.

The technical service staffs in most companies are very capable of recovering from many types of outages. After all, these are the very people who designed and built the system in the fist place! They know where every wire in the organization runs (well, usually) and have more committed to memory about their company than most of us could learn in a decade.

But what happens when key personnel are either incapacitated by the disaster, or maybe don't report for work ever again. After all, most have families which will be the primary concern after a major disaster. Would you come to work if your family was home alone, and your home was in danger of being looted?

One of my personal favorite ways to check the disaster recovery plan is to come into an organization and kill the LAN administrator. (No, not really – remember, it's just a test!)

The reason I like to pick on the LAN manager is that this key person phenomena is especially troublesome in distributed LAN environments. The point is, what happens to an organization's response when these key people are not available in a disaster? It's really interesting to see how the organization responds after the loss of a key player.

In light of these thoughts, it is important you present disaster recovery to your staff, not as some type of a quiz or test to prove they know their jobs, but in light of these facts, that other coworkers may be called to execute this plan. This means everything needs to be documented in a format designed to be easily followed by an outside technical person supporting the recovery efforts. Hint: Use a lot of pictures, a lot of diagrams, and spell out where everything is!

It's important for the people coordinating the recovery and response to know what was installed. Therefore, an important component to any recovery plan is an equipment inventory. At a minimum this should include:

- a listing of all equipment by type and model number;
- associated software packages, with version number;
- date of purchase; and
- original cost.

Other items are helpful as well, such as:

- name, address and telephone number of the manufacturer;
- and the local distributor or depot for the equipment.

Using this approach, quick command decisions are possible, even in the heat of the moment during a disaster. The more information on hand in a digestible format to provide rationale for these decisions, the better for the company and the decision maker.

Another item to consider is the software inventory, encompassing all software required for operation of all missing critical equipment. This inventory should include:

- the purpose of the software;
- the acquisition date of the software;
- the original cost of the software
- the license number; and
- the version number.

Other items which may find a useful place in an equipment inventory include such things as the location of third-party equipment suppliers. Since much of your equipment may be a few years old, it may already be seeing activity on the secondary market and be more easily acquired there.

Any mission-critical piece of equipment should have a disaster recovery plan, it behooves all to get this recovery plan from the vendor first. Such equipment should include things like mission-critical servers, mainframe computers, bridges, routers and gateways. The higher the price tag, the greater the likelihood your vendor may work with you. In any event, it is much more cost-effective to negotiate disaster recovery services with a vendor while they are actively after your business than to try to add these services later.

## "Importing" Data for the Plan

The best method for keeping track of equipment inventories, as well as other components necessary for the recovery process is through a process called "importing" data.

Importing means finding databases and repositories of information within the organization which you can reasonably expect to stay up to date, and then acquiring them for the plan, either manually, via magnetic media, or most preferably over a LAN. For example, when a piece of equipment is purchased, a document or file for the equipment is archived. Often times, the contract and the documentation to the equipment goes to accounting, where it's stashed away by the bean counters to be amortized. If you are lucky, documentation is stored on a LAN which may be accessible to you. The key is to locate and identify these repositories of equipment inventory data so they can be imported gracefully into the recovery plan.

Organizations which make heavy use of internetworked LANs have an advantage in importing data. Here it becomes relatively straightforward to import data from other departments connected to the same LAN. In this fashion, any time a file is updated, for example, in an accounting department, showing a new piece of equipment, there are a number of ways this could be automatically transferred without human intervention to a critical file within the recovery plan.

Object-linking Microsoft Word files, for example, is one way of doing this. By keying in on a specific file name, in this case in the accounting department, a technical service manager can be assured every time that department updates an equipment-list repository file, the file in his recovery plan will also be similar updated.

Maintaining up-to-date telephone numbers for personnel and critical equipment vendors is absolutely essential to the successful implementation of the plan, and similar methodology must be employed to ensure accuracy. Once again, this means importing data from reputable sources.

Consider home telephone numbers for employees. There are many places within the organization you can go to find a home telephone number for key employees; such as human resources and the company telephone directory. Human resources may be the best place to get this information. However, you may also find an employee who has worked for the company for 20 years still has the same address on file he had when hired. The company telephone directory may be a better bet in this case. The key is to identify, verify, then import.

Speaking of numbers, many others will be needed in the plan. These include telephone numbers for key equipment vendors and suppliers. Oftentimes, these can be found in the network control center, help desk, or other operational environments with day-today contact with these vendors. When telephone numbers for key vendors and suppliers change, these people are the first to know. Importing is best performed through object linking files together, perhaps in a LAN environment. It can also be accomplished through use of a Sneaker net and floppy disk. The important thing is it be done regularly, and preferably, without human intervention.

Consider importing components of the corporate-wide recovery plan. It makes little sense for a technical recovery planner to write procedures for such broad-based concerns as loss of a building, physical security, fire procedures, bomb threats, and other items which are company-wide in effect and scope. Indeed, as far as the make-up of the recovery plan, your recovery plan itself will probably end up being imported into a corporate-wide recovery plan for execution by an emergency management team. It works both ways.

## What Goes In the Plan?

Figure 1 illustrates one approach. We have used the concept of the Eight R's in many of our disaster recovery discussions. It serves as a good thought jogger and helps the technologist put tasks in perspective. It is also helpful to include a section of appendices at the back of your plan. This part of the plan is reserved for notes, detailed information, and things you will need but do not want cluttering up the main part of the plan. These can include:

- emergency call lists of management and recovery teams;
- vendor call out and escalation lists;
- inventory and report forms;
- carrier call out and escalation lists;
- maintenance forms;
- hardware lists and serial numbers;
- software lists and license numbers;
- team member duties and responsibilities;
- network schematic diagrams;
- equipment room floor grid diagrams;
- contract and maintenance agreements;
- special operating instructions for sensitive equipment;
- cellular telephone inventory and agreements; and
- miscellaneous (pictures of the kids?).

## Broad-based Document

There are a lot of good reasons for documenting a disaster recovery plan, and they will manifest themselves throughout the document. Your recovery plan will be a broad-based document, and will cover details which are company-wide in scope. It will contain statements which speak to the issue of:

- protecting life;
- minimizing risk to the company;
- recovery critical applications;
- safeguarding against litigation and shareholder suits;
- protecting competitive positions; and
- preserving customer confidence.

Disaster recovery plans are complex, and can ultimately take two years or more to complete. For this reason, don't be ashamed to ask for some outside help. While this can be taken in one way as an advertising plug from a disaster recovery consultant, it also comes from experience. In today's busy operational environments, disaster recovery planning usually becomes kitchen table work, if it gets done at all. Regardless of who does the work however, by understanding the components of a successful plan, and devoting an enthusiastic outlook to the project, you will be secure in the knowledge that you are not only protecting the interests of the company, but your long term future as well. Good luck.

## Figure 1: The Eight R's of a Successful Recovery Plan

**1. Reason for Planning**

Think of all the reasons your organization has for planning. There are many. Some common themes or sentiments can include:

- protect human life;
- recover critical operations;
- protect competitive position;
- preserve customer confidence and good will; and
- protect against litigation.

**2. Recognition**

What happens if someone spots water coming under the door to your equipment room at 3 a.m.? It probably will not be one of your people at that time of night. Do the security guards know who to call and how to report trouble? These are the kinds of concerns to address in the recognition phase:

- initial reaction procedures to a disaster report;
- notification procedures for police, fire, medical; and
- notification procedures for management.

**3. Reaction**

Once someone sounds the alarm, what then? Who handles security? Who talks to the media? Who is an employee and who is a looter? Careful planning here helps address these questions.

- mobilizing the EMT (executive management team);
- filing of initial damage assessment reports to the EMT;
- assisting EMT in preparation of statements; and
- opening a critical events log for audit purposes.

**4. Recovery**

- modified signing authority for equipment purchases;
- procedures for getting cash;
- procedures for maintaining physical security;
- procedures for arranging security at the damaged site;
- procedures for finding and getting to the recovery center (maps!); and
- procedures for arranging security at the recovery center

**5. Restoration**

- coordination of restoration of the original site;
- restoration of electronic equipment;
- reloading of software;
- restoration of power, UPS, common building systems;
- replacement of fire suppression systems;
- rewiring of the building;
- restoring the LAN; and
- restoring the WAN connections.

**6. Return to Normal**

- testing procedures for new hardware and software;
- what constitutes a successful test (before recommitting production);
- training operations personnel;
- training employees;
- scheduling migration back to original site; and
- coordinating return to original site.

**7. Rest and Relax**

- schedule compensatory time off; and
- make visits to employees in rehab from stress.

**8. Re-evaluate and Re-Document**

- review your critical events log;
- evaluate vendor performance;
- recognize extraordinary achievements;
- preparing final review and activity report; and
- aid in liability assessments.

---

***Note:*** *Portions of this article were adapted from Leo Wrobel's new book, Business Resumption Planning, available from Auerbach Publishers.*

*Leo A. Wrobel holds degrees in Telecommunications Systems Technology, Electronic Systems Technology and Business, and Public Policy. An active author, lecturer and technical futurist, Wrobel has published five books and dozens of trade articles on a variety of technical subjects. He possesses nearly two decades of experience and is president and CEO of Dallas-based Premiere Network Services, Inc.*