The Importance Of A Disaster Recovery Contingency Plan

Geoff Evelyn, Geoff@geoffevelyn.com, http://www.geoffevelyn.com

---

Every company, and each of its locations, is susceptible to disaster. Disk crashes, power outages, communication loss-are all minor disasters that happen on an occassional basis-and most of us have a back-up plan ready to put into effect. But what about major disasters fire, flood. That's why you need a comprehensive, effective, disaster contingency plan. Most companies are dependent on their computers to stay in business. But rather than just looking at getting the computer system set up, you also should be concentrating on how to continue the business. A disaster recovery plan really should be called a "business continuity plan" because the most important goal is that your business be kept running.

To determine your risk of a major disaster, ask yourself these questions: Are you in or near a building that has a potential for being attacked by a terrorist? Are you near a takeoff or landing runway of an airport? Are you near a major road? Are there tankers that carry nuclear waste or chemicals that may be toxic? All of these are potentials for disaster.

Employee Sabotage
The number one cause of computer centre disasters is employee revenge, sabotage and vandalism.

Strategies: change

Passwords, security lock codes, telephone PIN numbers

Get management to commit to it. The way to approach upper management is with a cost/benefit analysis. How can you justify it? What's the pay back? How much will your company lose on an hourly basis if the computer goes down? Find out what management thinks is important to include in a disaster recovery plan, and what new plans, if any, they are considering that may be important to implementing your plan.

The Recovery Process
The recovery process consists of the following steps:

1. **Identify Critical Products/Services**
Define your business, identify processing cycles and determine peak seasons, if any. Then develop your strategy. Every user department believes that its application is the most critical for the survival of the corporation. Depending on the business, this determination may change based on time of year. What are the minimum requirements to get the business back up, and how long do you have to get it up? The answers to these questions need to be determined as part of your recovery plan. Determine how long you can afford to be down. If you have a short two-to-four-hour window, you should have a mirror site where all your files are being shadowed. If you have more time you can either contract a "hot site" or within an eight-hour time frame you could develop your own hot site.

2. **Analyse Risks and Exposures**
You may have several contingencies built into your plan for how you are going to recover at different times of the year, depending on your peak season. Analyse your risk of exposure. If you could not bring a particular function up, what do you stand to

lose? Determine your communications needs-how many voice lines and data lines will you need? What will it take to get an application up and running? Determine in advance how big your communication network is, and how much of it you have to have up.

3. **Define Your Recovery Strategy**
When a disaster strikes, determine where you are in your processing cycle, and which application is the most critical at that time. There may be multiple recovery plans if you have a business of a cyclical nature. Many organizations are subject to government regulations. Determine what you need to do to be in compliance with state, federal and local laws. Remember the importance of maintaining the payroll function, especially if you are a union shop.

4. **Develop Detailed Recovery Plans**
Develop detailed recovery plans. Document them. Your plans should include contingencies for repairing or replacing existing equipment (hardware, software, telephones, cable, etc.), locating facilities within the building if it's a limited disaster, or a temporary location within a three-mile radius (a 100-mile radius in case of a regional disaster). You will need to know room dimensions; air conditioning, communication, parking requirements, controlled access; supplies-the list is endless-desks, paper, staples, all the supplies you need on a day-to-day basis. In the event of a total loss of the facility, you will need to know your floor space requirements. This estimate is critical because when planning for a new site for the computer facility you need to determine square footage, number of outlets, air conditioning, etc. Unless you have the latest technology, your floor space needs will be smaller. You will not be able to replace your hardware with exactly what you have now. Also be aware that your hardware platform may be different. Make sure your applications will run on that platform or operating system. You can go to the vendor and do some benchmarking prior to a disaster. It is time well spent.

Primary Vendors and Contacts
Your insurance representative should be your first contact. Read your contract. There may be a disaster clause in the policy that gives you an upfront payment. This will get you started. If you do not have a suitable plan, you may not be able to go to your vendors and order $3 million of replacement equipment to be delivered by the next day. If you have declared a disaster, they may require C.O.D. More disasters occur during off-hours than business hours. So be sure you have home telephone numbers, beeper and cellular numbers for all of your vendors. In the multivendor platform that most of us are in, you don;t just have one vendor-there are hardware vendors, software vendors, third-party vendors. List them all. But don't keep the list at the office, keep it in off-site storage!

And don't forget the cabling, networks, telephone-you need to be able to contact each company because you will need phone service very quickly.

Potential Vendor Contact List
Back up your back up. If it is a regional disaster, there is no guarantee that your vendors will be able to supply you with all you need. Make a back up list of potential vendors in other areas of the country. Call them ahead of time. Establish contact, find out what you need to establish credit.

One note of caution: Do not use the disaster as an opportunity to buy new hardware! It will cause more problems when you try to run your applications, unless you have already benchmarked. You may, however, need to do some upgrades to make a transition in a disaster easier.

And don't forget about licensing-be aware of any licensing requirements on any machine you may be running. Talk to your vendors to find out the possible migration paths. And arrange to have the appropriate license fees ready to be delivered on a moment's notice. Licenses are a key determination in a successful recovery.

5. **Test, Evaluate and Revise Recovery Plans**
Disaster recovery is a journey with no destination. You have a road map, but you're never going to get where you want to go because things are constantly changing. The list is endless of what could have changed since your disaster recovery plan was written-and all of them impact your ability to recover after a disaster. Test, evaluate and revise your plans as situations change. The key is to be prepared. By constantly updating your disaster recovery plan you will be ready when the unthinkable happens.

The Initial Post-Disaster Meeting

In a major disaster, where you lose your facility, you need to be prepared to have a meeting place where everyone on the disaster recovery team can get together quickly. It may be a home, a satellite office or a hotel meeting room.

But be aware that in a hurricane, tornado, or earthquake, highways may be blocked off. You may lose public transportation, and might not be able to get everybody together.

Tasks to be accomplished at the initial post-disaster meeting:

1. determine the scope of the disaster
2. select the planning team
3. review your products/services or critical applications
4. critically Analyse and prioritize operational functions
5. review exposures for each cost center
6. establish your recovery priority
7. determine the most feasible recovery options
8. determine facility needs and floor space requirements
9. set assignments, brief planning
10. break into assigned teams.

There should be some reports that come out of the disaster recovery meeting: an overview of the situation, what the disaster is, what it entails, what part of the plan is being implemented, who is responsible for implementing the disaster recovery program, etc.

Elements of a Disaster Recovery Plan

Every disaster recovery plan should include the following elements:

1. Introduction defining the disaster
2. List of Disaster Recovery Management Team names, addresses and home phone numbers
3. Primary vendors and contacts (names, addresses, home phone numbers, contract numbers)
4. Analysis of risks and exposures
5. Analysis of critical applications in order of priority
6. Overall resource requirements, including minimum resource requirements to get the business up and running
7. Management schedule
8. Job tasks and assignments

9. Potential vendor contact list
10. contact list
11. notification lists