

Developing a Comprehensive Disaster Recovery Plan

While an organization can never fully prepare for disaster, the fact remains that every operation is vulnerable to a wide range of disaster scenarios. Perhaps now more than ever, each organization should realize the importance of developing and implementing a disaster recovery plan. This plan should not only position an organization to quickly respond after a disaster, but should prepare an organization *before* the disaster so that the impact is as minimal as possible.

Gleaned from several sources, following are general guidelines in developing a disaster recovery strategy:

1. Recognize the need for recovery planning. Don't assume that disaster will never affect your organization. Recognize that a plan is critical, and it's part of everyone's job. Undoubtedly, an organization should plan for a disaster just as seriously as they plan for the future.

2. Establish a Strategic Planning Team. Ideally, you should pull together staff from every aspect of your organization to ensure that all interests are represented. This team will develop and implement the disaster recovery plan, and each member will serve as the head of their respective department's disaster team.

3. Identify disasters. The strategic planning team should begin by brainstorming to identify possible disruptive scenarios. From a water leak to a major natural disaster, jot down every possible 'disaster' your organization might face: disease epidemic, flood/water damage, fire/smoke damage, tornado, hurricane, earthquake, drought, blizzard, unexpected leave or death of a key employee, power outages/problems, leaks/water damage, unexpected influx in business, robberies, riots/acts of terrorism, loss of critical vendors, etc.

Once you have a good idea of the range of possible disasters, define three levels of disaster (minor, major and catastrophic) specific to your operation. Your definition might include amount of damage, recovery time, and how critical it is for your business to continue operating. Once you have defined what each of these three levels mean to your organization, each 'disaster' on your list should easily fall into a category.

4. Identify preparations. Much of the work in a disaster recovery plan is simply planning ahead – identifying areas or procedures that need improved before a disaster strikes, or taking preventative measures to protect the future. Some precautions to consider:

A. Protect your vital records. If you don't already have and enforce a rigid and regular backup procedure, NOW is the time to do so. Experts agree that you should always maintain at least two copies of every bit of data. At minimum, you should back up important files and immediately moving them to a safe off-site location for storage. Such a location should be remote enough to survive any disaster (such as a flood or tornado) that would affect the immediate area. (Beware that tapes are highly unstable, and images often deteriorate during storage.) And don't forget to occasionally test your backup medium to ensure that you are actually able to restore data from the backup files.

Similarly, your organization may elect to begin storing older records off-site now. Since prime office space is expensive, experts claim it should be used for people, not for inactive records. As a result, it may be cheaper to store records that are not actively used at an alternate location. Offsite records storage facilities should have: tested fire and smoke detectors, fire extinguishers and hoses, motion sensors, and active pest prevention efforts in place. Some storage entities even help organize and catalog documents, develop a retention schedule, duplicate and move originals, maintain records of what has been stored, and regularly remove and dispose of outdated records.

B. Review your insurance policy. Make sure your company's insurance coverage is sufficient, as you may need to purchase supplemental coverage. Pay special attention to "business income

coverage” (formerly called “business interruption coverage”). Some companies will even cover costs for helping displaced employees for up to six months after a disaster.

C. Maintain a thorough inventory. Ensure a thorough, well-documented inventory of all data, including systems, applications, hardware, network diagrams, furniture, fixtures, equipment, supplies, and employees’ task and responsibility requirements. After developing an inventory document, keep a copy of it store off-site, and be sure to update it at least quarterly.

D. Explore computer recovery and relocation options. While computer recovery needs vary depending upon the level of disaster faced, it is important to identify your options (and possible vendors), and which will be used for each level of disaster. Some options require contracts, and others require pre-disaster preparation.

To replace equipment at your site, the basic options include a vendor maintenance agreement or a quick ship program. Under a vendor maintenance agreement, the computer vendor is contracted to recover, repair and/or replace damaged or unusable computer equipment. A supplementary agreement may be necessary for certain situations (such as fire or flood). Under a quick ship contract, replacement hardware is delivered to your organization typically within three to five days.

In the event of some disasters, the organization may be forced to relocate. In this case, there are four basic options: cold sites, hot sites, mirrored sites, and mobile recovery facilities. A “cold site” is usually an empty computer room with basic electrical, environmental and support facilities in place, awaiting installation of replacement equipment. A “hot site” provides a fully operational, duplicate computer system in a prepared location with live, tested communication capabilities. A “mirrored site” is generally a separate location or office of the organization that contains all the hardware and communication facilities to assume operation, but perhaps with lower processing speed and capacity. Nightly backup tapes are often sent to the mirrored site and loaded, or data is transmitted to the site continuously so that the mirrored computers can pick up the workload almost seamlessly. Lastly, “mobile recovery facilities” allows you to bring the recovery location to your site via self-contained, trailer-mounted computer rooms, with equipment either preinstalled or delivered separately.

E. Other considerations. Also review your current information security and system access, physical security, physical environment housing computers, electrical power quality and reliability, fire detection and suppression, and current documentation practices.

5. Develop a disaster action plan. After taking any preparatory or preventative actions, the strategic planning team will need to focus on the specific plan of action to be followed if a disaster strikes. To accomplish this:

A. Determine who is responsible for initiating the disaster recovery plan. This person or team will need to quickly assess the damage, determine the level of the disaster, and put the recovery plan into effect.

B. For each level of disaster, outline responsibilities, tasks, timelines, and resources to address specifically how you will recover in the areas of customers, personnel, equipment, capital, time, IT infrastructure, and communications. (Start small by protecting applications everyone agrees are crucial, then broaden out to encompass other areas of your operation.)

C. Get other key agencies, organizations, and vendors involved in your plan. Talk with current vendors about their disaster recovery plans and level of commitment to customers during a crisis. Work with other agencies to share resources and ideas in the event of a disaster.

6. If disaster strikes... don't forget to take care of your employees first. As one industry leader pointed out, there is no use in saving the company if there is no one to show up and work. Depending on the level of disaster, employee needs will vary. Areas to consider include:

- Providing frequent updates about the status of the business' disaster recovery efforts
- Setting up a toll-free emergency number for employees and their families
- Coordinating any relevant counseling services
- Helping employees get back into their own homes or secure alternate lodging
- Offering flexible scheduling, casual dress codes, free meals
- If employees volunteer to work at an off-site location, allow them to bring their families, and provide free travel, lodging, and meals.
- Physical needs, such as food, shelter, blankets, and first-aid supplies
- Assisting in finding displaced family members
- Providing emergency cash, day care, emergency items, and a liberal leave policy
- If employees volunteer to work at an off-site location, allow them to bring their families, and provide free travel, lodging, and meals

7. Maintain, update, train. After developing a disaster recovery plan, don't just let it sit on a shelf. Distribute it to all personnel, ensuring that key staff have two copies – one for the office and one to keep in a safe, remote location. Review it quarterly, updating as necessary, and make sure all staff (especially new hires) are trained on their roles and responsibilities.

8. Test your plan. If possible, test your plan. Create scenarios, then walk through how it will be handled. Simply talking through the logistics will often uncover additional areas that need to be addressed, and can only help strengthen you plan.

SOURCES:

Bunetto, G. & Harris, N.L. (March 2001). "Disaster recovery: how will your company survive?" Strategic Finance, 57-61, 9.

"Agencies, too, must be prepared for disaster." (Nov 2000). National Underwriter, 104, 46.

O Herron, J. (April 2001). "Expecting the unexpected". Call Center Magazine, 50-57, 4.

Ohlson, K. (September 2000). "Guarding staffers from nature's worst." Computerworld, 54, 39.

Solomon, C.M. (April 1994). "Bracing for emergencies". Personnel Journal, 74-83, 73.

Romei, L.K., Fernberg, P.M., Malik, M. S. (January 1995). "Disaster recovery: are you ready?" Managing Office Technology, 26-32, 40.

Rothstein, P.J. (May 1998). "Disaster recovery in the line of fire." Managing Office Technology, 26-30, 43.