# Disaster Planning

BY REED BOOKER

Everyone who works with computers has nightmares of disaster. That's because computers and software are among the most fragile and sensitive of articles, and they are often as valuable, portable, and concealable as a diamond necklace. Computer disasters come in many flavors, including fire, theft and just plain failure. *ComputerWorld* estimates that one in 40 computer installations will suffer a disastrous event. The most common? Water damage resulting from someone else's disastrous event.

Owners of consulting firms and other computer-based enterprises must put disaster planning on their list of executive responsibilities along with obtaining work, performing the work, and collecting for completed work. All three functions depend on uninterrupted operation of facilities, equipment and manpower. Disaster planning should result in two action plans: disaster prevention and disaster recovery.

The first step to preventing a disaster is to imagine it: If something can happen, sooner or later it probably will. Steven Lewis, writing in a magazine about business insurance called *The John Liner Review*, identifies computer disasters in a typology of three: loss of data, loss of access to data, and loss of personnel.

Loss of data is pretty easy to comprehend. Hardware or software failure or damage has scrambled your information or erased it. This can happen through a variety of errors — human, mechanical or electronic, or through a variety of damaging events — the roof falls in, the circuit breaker doesn't pop, water pipes break, etc. And the damage doesn't always happen directly at your site. For instance, a skyscraper fire in Los Angeles destroyed several floors, and months later the cleanup of smoke damaged computers and media was still going on in a professional office located 10 floors away from the site of the fire.

**Hidden costs and losses are the primary reason that an estimated 43 percent of all businesses struck by disaster never reopen, and why 28 percent of those that do reopen close permanently within three years…**
**(Contingency Journal)**

At other times, the information may remain intact, but you can't get to it. The computers and software may be fine, but your floor is flooded and all your power is off. Or you lose a key employee, the one person who really knows how things work. This can be a devastating event for smaller companies where responsibilities seldom overlap. Those companies risk their success on the good health, good will, and continuing employment of certain key individuals. Or companies that depend on service bureaus for billing, receivables, and inventory records are at the mercy of disastrous events that may occur hundreds of miles away.

On the surface, disaster recovery would seem to be accomplished through a risk management program that transfers the potential risks to an insurance company.

## THE HIDDEN COSTS OF A DISASTER

It's true that all from the smallest to the largest companies can protect themselves with programs that cover the costs of restoring property and equipment, and they can even cover business overhead costs for many months. But business owners must also prepare to recover the hidden costs of a disaster. These uninsured losses include lost market share and momentum, increased costs of a restart that will include recruiting and training, lost relationships with vendors and clients, and many specific costs arising from unique experiences.

Hidden costs and losses are the primary reason that an estimated 43 percent of all businesses struck by disaster never reopen, and why 28 percent of those that do reopen close permanently within three years, according to *Contingency Journal.*

While covering the obvious costs of a disaster is the responsibility of the owner's insurance company, reducing the effect of those hidden costs is the responsibility of the business owner. How do businesses keep those hidden costs from shutting them down permanently? The answer lies in the ability of a business to regain productivity in the shortest possible time.

Nelson Bean, whose company Evans American Corporation of Dallas specializes in disaster recovery construction for large organizations, has found that hidden losses and costs of a disastrous event are time-related. Accelerating the recovery process — even though initial costs will certainly be higher — will reduce the longer-term costs of recovery and help assure continuation of a business. However, the only way to speed recovery is to have a solid plan in place well before a disaster occurs.

## SOLIDIFYING THE PLAN

The most important element of disaster planning is to define the responsibilities of individuals in the company prior to a loss. Planning is an ongoing process with periodic updates that will involve the staff in reappraising the threats to your company, keeping the plan current, and reminding everyone of their responsibilities.

Following is an example list of items that should be part of a disaster planning checklist for a small- to medium-sized computer-based enterprise:

***Recovering property and equipment losses.*** A staff member is responsible for acquiring property and casualty insurance to protect against specific losses due to, for example, fire, theft, water damage, power surges, computer viruses, even sewer and drain backup damage. Coverage may include both repair and replacement and loss of business income.

***Overhead costs during a key individual's recovery from illness or injury.*** A staff member, usually the owner or managing partner, is responsible for acquiring disability insurance benefiting the company.

***Maintaining important data in a separate location.*** This can be as simple as making backup disks to take home, or putting complete backup files in a safe deposit location.

***Planning a "quick exit and restart."*** Have an alternative location already picked out where hardware, software, and specific variables can be assembled and made operational within a few hours.

***Internal communications.*** Plan a flow of information to all members of the organization to keep them abreast of events and contingency plans. This will help maintain staff morale and motivation – the most important elements in working through trying times.

***External communications.*** Plan which persons will immediately inform key clients, customers, suppliers and affiliates about events, recovery plans and, most importantly, possible delays. Everyone outside the company will be more understanding if they feel you have leveled with them and given them reasonable expectations of service.

Remember, it's usually the nightmare you've never dreamed could happen that does. The best part about a disaster plan, then,is that the process itself helps business owners to identify potential hazards and risks, and through prudent action, prevent them from occurring. *ts*

**Reed Booker is director of association marketing of MIMS International, Ltd., an insurance program administrator serving NaSPA and its members. For more information on the types of coverage available, contact Debbie Zarzecki at (800) 899-1399.**