



Disaster Planning Post-Katrina: What's A Firm To Do?

Watching the devastation heaped upon the Gulf Coast was certainly a wakeup call for law firms and businesses across the country. Yet, studies show that fewer than 25 percent of businesses have a disaster recovery plan in place.

Still need some motivation to implement a formal disaster plan for your firm? Consider this fact: According to the Gartner Group, 40 percent of companies that experience a disaster are out of business within five years.

And a "disaster" doesn't have to be a category 5 hurricane, flood or terrorist attack. It could be any unplanned event that disrupts normal firm operations for a day or longer — anything from a major power blackout to a security breach or cyber crime.

"Okay, Where Do We Start?"

True disaster recovery planning starts by recognizing that there is a risk to your firm's physical facilities. This means *everything* in your facility, from "hard" assets (the building itself, computers, equipment, telephones and furniture) to data (both physically and electronically stored). From here, you can begin to assess the specific risks and make contingency plans.

The process of disaster recovery planning can be divided into two main components:

1. Devising emergency response procedures to help minimize the impact of damage immediately after the disaster. This focuses on getting critical IT systems and software applications back up and running as quickly as possible.

2. Formulating a plan to keep the firm functional in the weeks and months following a disaster. This includes steps for keeping critical business functions operational, such as restoring backups and implementing procedures necessary to ramp back up to pre-disaster business levels as quickly as possible.

“What’s At Risk?”

The first step in creating your disaster recovery plan is to identify possible risks and quantify their potential impact on the firm’s critical operations and systems. Based on this, you can determine which operations and systems should receive the bulk of recovery resources, and how quickly this has to happen. Systems may be classified as follows:

Critical — These are functions that the firm cannot operate without and that can’t be performed until they are replaced by identical capabilities.

Vital — These functions could be performed manually, but only temporarily.

Sensitive — These are functions that can be performed manually at a tolerable cost for an extended period of time without seriously impacting the business. However, this may require hiring additional staff to perform the functions.

Non-critical — These are functions that may be interrupted for an extended period of time at little or no cost to the firm.

“Who Should Be On The Team?”

Next, determine staff members who are key to restoring your critical systems and then designate the team that will manage your recovery efforts. This team’s responsibilities should be planned in detail. For example:

- Who will notify employees not to report for work, or to report to another site?
- Who will see that critical data is retrieved from an off-site storage location?
- Who will communicate with clients, the media and government officials during the crisis and its aftermath?

“Who Has The Calendar?”

The first priority is to make sure you have your data backed up *somewhere* off-site. Depending on how urgent the data is, you can opt for inexpensive traditional media storage or more expensive electronic storage.

For some firms, it may make sense to contract with companies that specialize in providing disaster recovery services. These services include disaster recovery hot sites — physical locations where employees can come to work — redundant data storage, and secure hosting services for both Web- and non-Web-based applications.

One area that is often overlooked in disaster planning is the firm’s calendar. Imagine the impact on your firm if even one attorney loses his or her calendar carried on a personal laptop or portable handheld device — let alone the calamity and interruption caused by losing the calendar for the entire firm. If you have not already, consider running a centralized calendaring system and maintaining a tape backup.

“Where’s The Plan?”

Your disaster recovery plan should be a formal written document that is stored in a secure location (preferably off-site) and updated as circumstances warrant. As part of your plan, develop and maintain a list of key contacts, including families, insurance companies, clients and suppliers.

Distribute two copies of the complete plan to all key employees: one copy for home, one copy for the office. And distribute disaster recovery information to all employees in the form of wallet cards or other means that are easily accessible.

Regularly reviewing your plan on paper is important, but it is not enough. In addition to tabletop tests, consider springing mock disasters on your disaster recovery team, requiring them to set up a duplicate office offsite so that it is operational within a few hours.

“Are We Covered For That?”

Your analysis should also include a careful review of your insurance coverage. Business interruption coverage is usually included in most standard small business insurance policies.

Partners need to go back and review their actual loss of income and extra expense coverage to make sure they’re adequately covered for whatever

period they determine the firm might be down. This is the working capital that will sustain the business during this time, so it's vital. Likewise, the firm should also have access to a line of credit it can draw upon until it's up and running again

“Isn't It Going To Cost A Bundle?”

Creating a disaster recovery plan doesn't have to be an expensive or time-consuming process. Many of the steps in your plan will involve simple, common-sense things that you and your employees should do, like making sure supervisors have current home phone numbers for all their reports and maintaining a closet of emergency supplies on site (e.g., food, water, flashlights and a source of communication).

Other steps will involve very detailed and technical processes to safeguard and ensure access to data and secure an alternate physical facility where employees can come to work.

The bottom line is that no one knows when disaster will strike — but you can prepare your firm to weather the storm.