# PREPARING FOR AND RECOVERING FROM DISASTER

Ellen Freedman, CLM


---

> *Preparedness is everyone's job. Not just government agencies but all sectors of society—service providers, businesses, civic and volunteer groups, industry associations and neighborhood associations, as well as every individual citizen—should plan ahead for disaster. During the first few hours or days following a disaster, essential services may not be available. People must be ready to act on their own.*
>
> *Federal Emergency Management Agency*

All eyes in the nation recently focused on the plight of gulf coast residents whose lives and businesses were abruptly altered by Hurricanes Katrina and Rita. The quote above, from the FEMA website, has appeared on the opening slide of my seminar on Disaster Prevention and Preparedness for a several years. Yet, in the devastating aftermath of these recent events, FEMA has come under fire despite its warnings. The inevitable investigations will not change the indisputable fact that that the worse the disaster, the longer it takes agencies to respond appropriately. You need to be aware of that when crafting your disaster prevention, preparedness, and recovery plans.

According to the U.S. Bureau of Labor, most businesses that experience a major disaster are no longer in business within five years. The Hartford Loss Control Group figures indicate that fifty percent of businesses that experience a major disaster are no longer in business within two years. Sadly, both consistently estimate that 75% of U.S. businesses do not consciously prepare for disaster recovery.

Disasters come in many forms. I categorize causes of disaster into four broad categories:

**1: Natural Disasters**

| | | |
|---|---|---|
| Earthquake | Heat wave | Fire |
| Flood | Hurricane | Landslide / mudflow |
| Tornado | Tsunami | Storms / wind / lightning |
| Wildland fire | Blizzard / ice storm | Volcano |

**2: Technological Disasters**

| | | |
|---|---|---|
| Equipment failure | Noxious or poisonous fumes | Nuclear power plant emergency |
| Sewer main break | Water main break | Power outage for extended period |
| Heat or air conditioning outage for extended period | Storm sewer backup | Hazardous material spills |

**3: Man-Made Disasters**

| | | |
|---|---|---|
| Sudden death or disability of firm partner | Intentional or accidental deletion of files and forms | Bombings, bomb threats, acts of terrorism |
| Computer crimes | Workplace violence | |

**4: Human Error**

Disasters caused by human error are too numerous to list. Consider that a single failure in a power transmission system near Cleveland, Ohio turned into a cascading failure that knocked power out across much of the North-eastern US and Ontario on August 14th, 2003. More than 50 million people were without power, from Michigan all the way to New York City and most of Ontario, Canada. The cascading failure was caused by human error. Human error also accounts for accidental deletion of computer files, downing of computer systems, severe lapses in security, fatal airplane crashes, fires, disabling or fatal car crashes, and more.

Loss control data indicates that 2% of disasters are intentional / man-made, which can affect the firm principal(s), or the firm as a whole; 5% are caused by natural disasters, which can affect an entire region; 25% are caused by technological failures; and the largest percentage of disasters, 68%, are attributable to human error.

Although man-made and natural disasters combined account for only 7% of disasters statistically, these are the types of disasters which can affect not just the firm, but your employees, your clients, your service providers, and even the region as a whole. It may become even more difficult to recover therefore, when those you count on both inside and outside of your firm may be similarly affected and therefore unavailable or ineffective, and as emergency resources are both diverted and strained to the limit. For this reason I believe that your prevention and recovery planning should begin by focusing in these areas. Fortunately for you, we have learned much about what to do, and what not to do, from the unfortunate experiences of gulf coast law firms.

Disasters can also come in unusual and unexpected ways, too. I once worked for a firm which was affected by a sewer main break nearby. It inundated the building with festering foul liquid, cresting at five feet. Believe me, it was a true disaster, with all the associated disruption and loss, in every sense of the word. Even an extended power outage when a deadline is looming large can have a severe adverse impact on the firm's ability to render timely service to its clients.

When it comes to disaster, reaction after the fact is no substitute for planning beforehand. I am constantly amazed at the number of attorneys who do not practice the most elementary form of disaster prevention — backing up the critical information on their computer system daily and taking that back-up off-site every night. Foresight and planning can make the difference between your practice surviving a disaster, or not.

As you design your plan, always keep these two goals in sight:

- GOAL ONE: Assure the safety of your people, and their recovery in the event of a disaster which impacts them, first and foremost.

- GOAL TWO: Restore your ability to delivery service to your clients.

Your overall plan should be regarded as a work in progress. It will evolve as you slowly identify and plan for each type of disaster, and make appropriate plans for recovery from each. Your plan must be constantly re-evaluated and tweaked as the firm changes from growth, contraction, change or addition of locations, changes in insurance coverage, and as people come and go. Don't plan on creating a plan once and leaving it on the shelf to collect dust. It must be consistently and effectively communicated, and should be reviewed for possible changes annually.

To develop a plan, three steps are required. First, identify every type of emergency which might affect your firm. Geographical location, size, and other factors, such as proximity to railroad lines, airports or nuclear power plants, will affect the final list of potential emergencies. Sort and prioritize your list, based on seriousness and type of disaster. Second, for each identified disaster or type of disaster, create a comprehensive checklist of what steps must be taken to a) prevent the disaster if possible; b) assist employees to recover from the disaster; and c) regain the ability to service clients. Three, determine specifically who will be responsible for accomplishing each item on your checklist, including a back-up individual or vendor, and what resources will be available to accomplish the task.

First, let's dispel some assumptions we know no longer work. Before 9/11, it seemed safe to assume in your disaster recovery plan that your building would still be standing, especially if it was a skyscraper. It seemed safe to assume that it would be easy to contact employees by telephone or computer to determine that they were safe. Before Hurricane Katrina, it seemed safe to assume in your disaster recovery plan that your city would still exist. It seemed safe to assume that lost client records could be re-created with cooperation of other counsel, courts, and clients. It seemed safe to assume that a back-up of a computer system, stored at a separate physical location in close proximity to the office, would be sufficient to recover essential business information. We now know that good disaster recovery planning requires a serious questioning of all assumptions.

For most types of disaster, excluding those which affect firm principal(s), there is a universal to-do list. Here are some of the things you need to think about and plan for:

1. ***Notification to clients, employees and vendors:*** without access to your office, do you have the names, addresses, email addresses, and phone numbers of your clients handy? Can you quickly get in touch with all your employees to keep them informed and make sure they're ok too? Do you

have emergency contact numbers for each of them accessible? Can you contact your vendors for emergency assistance? If your vendors are also affected, who do you call as a backup?

If you use something like Outlook or GroupWise personal productivity software for all your contacts, or a case management package which has a PDA interface, you can keep the information on a hand-held device for quick access. You should also print a master list and keep it off-site. If you use the print method, remember to do it regularly, like once a month or at least once a quarter. Put it on your calendar so you don't forget. Make sure a copy is kept in a different geographic location. If you have a branch office, swap information.

2. ***Access to firm documents, and client files:*** Let's start with clarification. Backup is about restoring your data. Chances are, if you're doing so, you need to do it quickly and thoroughly. You need to get back to the precise point you were at before your information, including software with all of its patches and customizations, was trashed. It is not about saving time or money when doing your backup. It's about regaining the essential information and systems you need to service your clients as quickly as possible when necessary. That means you should never ever do anything that interferes with achieving that goal. No incremental backups. No backups of just data. You want an entire backup of your system done each and every day.

   Thanks to drops in hard drive costs, I recently migrated from a tape-based system to an external hard drive. For under $150 each, I got two 80 GB hard drives which are very small and weigh under 3 pounds each. One is stored at my mother's residence, sufficiently far enough away to survive anything which might affect me, but close enough to get back if I need it. I rewrite a complete backup to it monthly. The other sits atop my file server and is automatically backed up to nightly. No more tapes to buy, at a cost of over $40 each. No more thinking about, or forgetting, swapping tapes. And finally, as my fail-safe, I have started on-line backups weekly. Again, this happens automatically without intervention on my part. [Contact me for my resource on hardware, software and on-line back-up resources.]

   If you have been smart enough to make a regular back-up of your computer system, and take it off-site every night, you will probably have access to all

the form documents and client documents you created. If in addition your office has worked to embrace the "paper-less office concept" by scanning in as much of incoming documents as feasible, keeping telephone messages electronically (e.g. unified messaging), getting depositions on disk and transferring them to your file server, using case management, and so forth, you will have access to most or all of the contents of your client files, even if the physical file is inaccessible or destroyed. (After the Meridian Bank building fire in Philadelphia, for example, law firms whose offices were not significantly damaged still could not gain access to retrieve their files for quite some time while it was being determined if there were building structural problems.)

Of course, what we learned from Katrina is that the back-up stored off-site may be no safer than the computer itself. So you should consider either sending a back-up to a branch office, a vacation home, or creating an electronic back-up to a secure e-vault. Some of the pluses of internet backup are that they are automatic, stored off-site in a different geographical region, and recoverable by internet connection from anywhere. No need to physically get to the back-up you've left at your vacation home in the mountains. The down side is that even with a broadband connection, depending on the size of your server's hard drive, the time required to back-up electronically may be prohibitive.

Keep in mind that having a current back-up tape off-site is one thing, but having a computer capable of restoring the data (meaning compatible operating system and sufficient disk space) is another. Some forethought has to go into that, or you need a good vendor relationship you can count on in a crisis.

3. ***Access to insurance records:*** Very few people think to keep a duplicate copy of their critical business insurance policies, or medical and other benefit policies, in a location outside the office. When the office burns down or washes away, and you want to know your coverage, it isn't very helpful if the policy is lost too, is it? Your agent can speak to your coverage, but waiting for a duplicate copy of the actual policy to arrive, should there be any disagreements, can take quite some time.

4. ***Appearance on behalf of clients:*** What critical dates are looming? Few people physically keep their calendar in their pocket anymore, unless it's

stored in a PDA (personal digital assistant). If you don't computerize your calendar, so as have it on your off-site back-up tape or on a PDA, how will you know what deadlines are coming up?

5. ***Cash flow issues:*** How will you record time, collect your receivables, and bill out your inventory? Will you know what is owed to you, or depend on the kindness and honesty of clients to send in their checks? Will they hold back payment because they are not sure where to send checks? If you are using a time & billing system, it also should be backed up, with the back-up stored off-site, so that you can restore it if necessary to gain access to critical financial records. Do you have business continuity / interruption insurance?

For disasters which affect firm principal(s), caused by sudden death or disability, plane or car crash, or other causes, there is a different set of considerations. There are lots of indispensable people in our lives. But often we don't know it until they're gone. Your firm needs to think about those who are essential to the proper management of the firm, or its financial success, and create a plan which can minimize the impact of their sudden loss.

If you are the sole principal of the firm and become seriously and suddenly disabled, you need to think about and plan for the following: Who will write checks? Who will have authority to sign checks? Who can deal with your escrow account and disburse payments if necessary? Who will make sure that your rent and insurance premiums are paid? Who is designated to step in and temporarily handle deadline work for clients? Are they cleared for potential conflicts? Who will pay your staff, and if necessary deal with the media and/or notify clients on your behalf?

You don't want to emerge from a coma only to find your client base eroded, your trusted staff gone, your insurance coverage cancelled, and several malpractice cases pending due to missed deadlines. Even if you have one or more partners, don't assume that they can access all the necessary accounts or information without preplanning. Have they been included as signatories on any individual interest-bearing escrow accounts you've established? Can they get to your calendar to anticipate deadlines? Can they access all documents, or are some passworded, or hand scribbled and indecipherable?

At a minimum your plan should probably include these 13 items:

1. Disability insurance
2. Business overhead expense insurance

3. Durable General Power of Attorney for bank accounts
4. Durable General Power of Attorney to sign tax returns
5. Power of Attorney form for each financial institution or brokerage firm
6. Specimen Signature Designation in a Qualified Retirement Plan
7. A document or letter describing the basics of running your practice, which is updated annually. This would include information on how your filing and calendar systems work, business debts and when you pay them, your client list, payroll information, landlord and rent information, and so forth.
8. Your computer passwords
9. Your ID numbers: PA, SSN, FIN
10. Names and addresses for critical people like accountant, attorney, insurance carriers
11. A Will
12. Designation of a personal representative with the power to continue to operate your firm during the administration of your estate
13. Someone who agrees in advance to be attorney in fact and conservator
14. "Hit by a bus" detailed list of essential duties and information, to be created by each key administrative employee

This is not by any means a comprehensive list. It should, however, get you started thinking in the right direction about where you are vulnerable, and what you can do to plug up the holes. Fortunately, there are excellent reference sources to turn to. Pennsylvania Bar Association members are encouraged to contact me for additional information and resources.

## RESOURCE LISTING

**Available through the Association of Legal Administrators at 847-267-1252 or www.alanet.org**

"Managing Emergency Situations in Law Firms: Minimizing the Damage" by Nina Wendt and L.J. Sklenar

"Emergency Management for Records & Information Programs" by Virginia A. Jones, CRM and Kris E. Keyes

"Disaster Survival Planning: A Practical Guide for Businesses" by Judy Kay Bell

**Available through the Pennsylvania Bar Association at 1-800-932-0311 or http://www.pabar.org/pbastore.shtml**

"The Essential Formbook, Volume IV, Part 1" by Gary A. Munneke and Anthony E. Davis

**On-line Resources**

"Disaster Recovery Yellow Pages"
http://www.techstreet.com/cgi-bin/detail?product_id=1095225
or
http://www.disaster-help.com/toc.html

Edwards Disaster Recovery Directory
http://www.thedryp.com/

Wikipedia on Disaster Recovery Planning
http://en.wikipedia.org/wiki/Disaster_Recovery_Plan

Managing Practice Interruptions by Dan Pinnington
http://www.practicepro.ca/practice/Practice_Interruptions_booklet.pdf

University of Toronto's Disaster Recovery Outline
http://www.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm

A Disaster Recovery Checklist by Hewlett Packard
http://www.hp.com/sbso/solutions/legal/expert_insights_disaster_recovery.html

Disaster Recovery Journal
http://www.drj.com/

Disaster Recovery World Online
http://www.drj.com/drworld/content/special.htm

Sungard's White Papers
http://www.availability.sungard.com/Resources/White+Papers/

Dennis Kennedy's Disaster Recovery Planning Handout from ABA TechShow 2005
http://www.denniskennedy.com/kennedydisasterrecovery.pdf

Protecting Your Computer
http://www.pa-lawfirmconsulting.com/pdfs/technology/PROTECTING_YOUR_COMPUTER.pdf

Getting Started: Disaster Recovery Planning
http://www.disasterplan.com/yellowpages/intro.html

*A version of this article originally appeared in the January/February, 2006 issue of The Pennsylvania Lawyer*



Freedman Consulting, Inc.
(215) 628-9422