

# Disaster Preparedness: What's Reasonable?

By Sharon D. Nelson, Esq. and John W. Simek

© 2006 Sensei Enterprises, Inc.

---

## The Call=Chronicle=Examiner

SAN FRANCISCO, THURSDAY, APRIL 19, 1906.

---

# EARTHQUAKE AND FIRE: SAN FRANCISCO IN RUINS

---

Disasters are not new. The great San Francisco earthquake of 1906 was, in its time, a disaster greater than Katrina. 3000 people perished. The city burned for four days. Virtually all law offices in the city were destroyed. All of the lawyers' data, being paper, was reduced to ashes. The 1900 hurricane in Galveston, Texas took more than 8000 lives. They didn't name hurricanes back then, but this one proved to be the greatest natural disaster in the history of the U.S., hitting the island city of Galveston with 150 mph winds and a 16 foot tidal wave, which submerged the entire island. Many of the city's lawyers died – all lost their practices. Can we ever prepare for such disasters? Probably not. Instead we look to find some standard of reasonableness to follow.

Katrina was not reasonable. No one expects a single disaster to take both your home and office – and to leave your business and family in shambles. With few exceptions, the 6000 lawyers who lost their offices because of Katrina were woefully unprepared. The primary exceptions were large firms, with well-developed and executed disaster recovery plans. Curiously enough, the September 11<sup>th</sup> terrorist attack presented a more rational disaster for which to prepare, one that didn't involving wiping out an entire geographic region. Both of these modern disasters, awful as they were, have been instructive. It has become more and more clear that there are relatively simple steps you can take to minimize the disruption to your law practice should disaster strike.

### **Start with the Basics**

One thing we all learned as children was not to leave our chocolate bars on the porch in the summer sun. Why? They would melt quickly and become a big, ugly and inedible mess. The recent storms in the gulf coast have also taught us a fundamental lesson. Don't leave all of your important paper records in the lowest part of the building – the basement. Gravity is relentless! Water will find the lowest point and move up from there. As the water recedes, the greatest damage will be to anything stored below ground level, which will have been soaked for the longest period of time. Don't forget about the possibility of fire damage too. Besides the obvious effects of fire outbreaks, fire fighters

will use water to combat the blaze, so you may have to simultaneously protect against the twin hazards of fire and water.

It's all about risk assessment. One of the first steps in preparing for some sort of failure is to assess the likelihood of the failure in the first place. Will a falling meteorite crush your office in the next several years? Not likely, so why plan for it? Plan for the probable failures first – loss of power, hard drive crashes, and mischief caused by hackers and disgruntled employees. Start small and work up from there. Sad to say, any law firm would be well advised to be prepared for a terrorist attack of modest geographic impact. Ditto for fires and floods, which are a fact of life, though generally much less devastating than Katrina. One by one, here are the chief points to consider in disaster recovery.

## **Data Backup**

The first thing that you should consider is the integrity of your data. This doesn't necessarily mean disasters like Katrina, Rita or Andrew are in your future. It is said that over 97% of information is electronic and will never make it to paper. This means that there has to be adequate protection for the electronic data storage. As an example, you need to plan for recovery from a virus infection, which could render your data inaccessible. In addition, a disk failure would make your data inaccessible as well. The point is that storms are not the only failures to plan for.

Perhaps your server is in a closet along with the water heater for the office. What would happen if the water heater developed a leak? Is the server high off of the ground and out of the path of any water leakage? Falling rain and rising floodwater are not the only considerations when planning for disaster. Besides the obvious considerations for leaking pipes and the like, don't forget to be aware of leakage from air conditioners. Air conditioners condense the moisture out of the air and drain it away. We've seen situations where an overhead air conditioning unit was in the room with the server. The condensate drain clogged allowing water to overflow onto the server and the telephone switch. Fortunately, the circuit breakers tripped. No data was lost as drying out the power supply allowed the server to restart normally. The point is that no one considered the air conditioner to be a source of potential problems.

So what are some of the methods and considerations for data backup? Certainly tape backup is very common. When using tape technology for backup, don't forget to do test restores on a periodic basis to ensure that the data is really getting backed up. Also, tapes do fail after constant usage and should be replaced. A good rule of thumb is to replace tapes annually. The cost of new media is very small compared to the loss of data if the tapes fail. Finally, store backups off-site in a safe place. We are still hearing stories of those in New Orleans that did have off-site storage, but still lost the data, as the off-site facility was also flooded. Perhaps it is unreasonable to anticipate such a catastrophic situation as Katrina, but that is a personal decision for each of us. If you are particularly paranoid about losing your data in a truly catastrophic incident, you can make an arrangement with a family member or colleague in another state and send periodic

backups to them for storage. Again, it is a personal decision and you must weigh the cost and effort against the likelihood of a major disaster.

Another good alternative for data backup is using an external USB hard disk. This is a great alternative for a single computer or the main data storage in a peer-to-peer network. When using external USB disks, get at least two of them so that you can rotate off-site storage. The external disks are fairly fast at data transfer and very simple to use. Like the tape alternative, do periodic test restores to verify that the data is really getting backed up.

Another alternative is to use an off-site storage service. Typically, these services backup your data to their servers and use the Internet to get it there. We don't recommend that you trust your data to a third party provider unless you encrypt the data before handing it off. This adds another step to the backup process, but will ensure the confidentiality of your client information, as **you** will hold the encryption keys and not the third party vendor.

## **Software**

You'll need to secure the media for your software applications too. Make sure that you have any update files for the applications as well. This will allow you to reinstall your software and get it to the same level as before the disaster.

## **Power**

Computers need electricity, so your disaster plan must account for the loss of power. As a minimum, you should have UPS (Uninterruptible Power Supply) devices for your computers to facilitate an orderly shutdown. You can also operate your computer for a short period of time on these battery-based units if they are large enough. If you need to sustain operation for a longer period of time, you will need to consider having a generator to supply power. This may be a simple portable gas generator or a large fixed diesel generator. Calculate the anticipated connected load and size your generator accordingly. Generators will not run forever and need fuel to operate. Make sure you have sufficient fuel available to operate the equipment. Test the generator on a periodic basis and actually simulate a power outage.

Don't forget to consider office lighting when you size the generator. There may be areas of your workspace that do not have natural light and therefore need lighting. This will add to the connected load. Printers are high power drain devices too. When running your tests, don't just plug in all of the devices. Make sure you actually operate all of the equipment simultaneously as you would in a real disaster.

## **Communication**

You may need to consider communication failures as part of your disaster plan. Assess the likelihood of cellular failure. Communication companies will get their services

operational as soon as possible, but you may need an alternative until that happens. For critical operations, satellite phones may be in your future. Don't forget that these devices need power too, so include them in your power backup plans.

Do you need to transmit data during a disaster or is voice communication good enough? Make sure that your backup communication plan can accommodate data transmissions if needed.

### **Configuration Values**

Perhaps the one exception to the storage of electronic records and data is something we'll call configuration data. This would include things like passwords, logons, account numbers, etc. The critical bits of information that you would need to recover should be printed to paper and kept in a waterproof and fireproof location. As an example, you may need your insurance policy and your agent's phone number to get the ball rolling following a disaster. You may need to purchase a new computer and need to reinstall your application software. Installation key codes, registration codes, vendor support phone numbers, etc. are all things that should be included as part of your "configuration value" kit.

### **Have a Plan, Review the Plan, Follow the Plan**

In small law practices, it is painfully apparent that there is often no disaster plan at all. No matter how small the law firm, there should be a disaster recovery plan, with an easy to follow checklist. Plans will stagnate over time as technology and other circumstances change, so they should be reviewed at least annually. Finally, make sure your "emergency to-do checklist" is with you at all times. Disasters don't knock before they come in.

*The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone)*  
[www.senseient.com](http://www.senseient.com)