WHEN THE DAM BREAKS: DISASTER RECOVERY AND BUSINESS CONTINUITY IN THE DIGITAL AGE

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

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.

Some of the most instructive disaster recovery lessons of our time have come from Hurricane Katrina. Not only were law firms felled en masse, an entire city failed to function. For those legal assistants, paralegals and lawyers who may be involved in disaster recovery planning for their law firms or other legal entities, one of the very best places to start is with the lessons of an unrelenting lady named Katrina.

It's hard to believe that it has been almost nine years since Hurricane Katrina struck the Gulf Coast with such magnificent force, destroying all that lay in the path of one of Mother Nature's most turbulent creations. The surging waters were no match for the outdated levy system and poured into the streets of the coastal towns with tremendous force. The one hundred twenty five plus mile per hour winds knocked down buildings, communication towers and other critical structures. After the storm had subsided, nobody knew what to do. Utilities were gone. Law and order was only sporadically in evidence. Everyone was searching for loved ones and waiting for permission to re-enter the cities that had been

evacuated. Chaos ruled. But almost as soon as Katrina subsided, the recovery effort began.

In New Orleans, one of the cities hit hardest by Hurricane Katrina, signs of the struggle to recover from one of the nation's most powerful disasters began to emerge. The surging waters had flooded and destroyed critical infrastructure vital to the success and speed of the recovery efforts. The powerful winds knocked down and destroyed most of the cell towers in the area. Landline phones were dead. Relief and rescue workers, fire and police departments, and other personnel could not communicate with their radio networks using incompatible frequencies. The system designed to bridge the various frequencies failed when the telephone switch that they relied on malfunctioned. Communication with the outside world was temporarily all but impossible. Even the Mayor of New Orleans, Ray Nagin, was affected by the lack of preparedness. He was unable to communicate about the relief efforts with the White House, but with a little improvising, an Internet connection at a hotel outside the city and a Voice-over Internet Protocol (VoIP) phone, he was finally able to reach the President aboard Air Force One.

Many businesses (including law firms) and the city of New Orleans were not prepared for disaster. With the benefit of hindsight, it quickly became clear that the disaster recovery plan that was implemented relied on older technologies that were outdated, unreliable, and filled with misguided assumptions about the ability of critical infrastructure to survive and operate after a disaster. The many failures of that plan provide us with lessons that can be learned from when designing and implementing our own disaster recovery plans today.

The more recent Hurricane Sandy of 2012 showed us that while our technology has improved, we were still unprepared for extended failures of our infrastructure. This time the cellular carriers were better prepared with portable temporary cell towers. However, the loss of electrical power severely strained businesses and law firms in their attempts to continue operations. In fact, the concentration, understandably, was to protect lives.

The best way to address the problems created by disasters is to plan for them to actually occur, no matter how unlikely they may be. Simply put, disaster recovery is a plan that defines resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. A disaster recovery plan should be part of an overall business contingency plan to keep the business operational during a disaster. This also applies to governmental agencies, which really are just specialized businesses.

It is essential that the right people are involved with the planning and development process from the beginning. Firm management, IT, legal assistants, paralegals, lawyers and any other classification of impacted employee - they should all be involved. Sometimes, law firms balk at including legal assistants or paralegals. They often do not see them as fundamental to the process. They are, of course, wrong in this assessment. Legal assistants and paralegals are often the employees that keep the firm running after a disaster. They know the ins-and-outs of the day-to-day operations and can address some of the questions that any disaster recovery plan must answer. They are the employees who know everything from whom to call if the printer is broken to what time you are due in court. Lawyers are often all but helpless without their support staff. They are integral to proper preparedness and formation of a disaster recovery plan and team. The most common failure after a disaster occurs is a communications failure. Who has the emergency contact list? It's great if it is on your server, but what happens when the server goes down? Is the list synchronized with your smartphones? Are there print copies in the hands of all the critical people? At home and at work? The disaster recovery planning should start from the ground up and involve the entire organization. Partners should establish their own plans as well as managers of each department, and should solicit help from others if needed. In the end they should incorporate all of the plans together into a global disaster recovery plan for the firm.

The point is simple; a law firm or any other business must involve all key employees in the development and planning process of the disaster recovery plan so that all may be prepared in the event that a disaster strikes.

Planning for Disaster Recovery

”Disaster recovery plan” can’t simply be a throwaway phrase with a quick fix solution. This is not a “one-meeting and we’re done” drill. Developing a workable plan takes sustained effort and serious thought. Each and every aspect of the firm’s operation needs to be reviewed and documented. Here again, the support staff actually know what goes on in the office and frequently do much of the documenting. From appointment scheduling to the billing system, document storage and client files, everything will need to be considered in the context of emergency readiness.

We often counsel clients to be rational. Should you prepare for an alien attack? That’s probably a little extreme. Should you prepare for a terrorist attack? Today, certainly. Likewise, you need to prepare for extended power outages, fires, floods, hurricanes, and the like. We should also mention “data breach” as another potential disaster, but that would consume another entire article!

One of the most important questions that you want to ask yourself when working on a disaster recovery plan is: What is our threshold for pain? How long can the firm be down? Cash flow can become a big issue after a disaster strikes. It’s necessary for the survival of the firm to get the employees putting billable hours on the books so that bills can continue to be paid during the recovery process. Support staff can play a vital role in assisting attorneys getting back on the ‘billable’ track. They can help with scheduling, contacting important clients, and organizing files and communications during the recovery process. This will allow the attorneys to focus on their clients, keeping them happy and paying! What will you do if the banks are closed? The firm doesn’t want to be short when it comes time to distribute employee pay checks. As Katrina taught us, most spectacularly by the airlifting of monies from Texas into New Orleans, that is not just a theoretical possibility.

The first step is to form the team, including representatives from IT, Management and support staff. After that, here are some of the first steps to be taken:

(a) **Be Organized** – Simple statement, hard to put in practice. We have all seen what many attorney offices look like, with their haphazard and

precariously perched stacks of paper. Files in cabinets and boxes of documents populate many a law firm's storage area. That's ok if they are all organized and documented, but often they are not. Organization of the mess will bode well for successful disaster recovery. Who will lead a disaster recovery effort and what will the firm do if that person is not available? Everyone needs to know and understand the organization of the plan, who to contact, who is in charge, where to meet, how to communicate, etc. Organization is a key factor to quickly getting a firm or business back up and running. You should designate and educate groups of people to carry out certain tasks during the recovery process and not just leave a task up to one person. That way if someone cannot be located, you can rely on other people in the firm to complete the task. It is important to involve everybody.

(b) **Show Me the Money** – Can't you feel your pockets becoming lighter already? The bottom line is that, once you have preserved life, it's all about getting back to business and making money. Imagine what a crisis the firm would have on its hands if it was shut down for a week or two and wasn't able to generate any incoming revenue. If you can't continue to bill and generate revenues, you will most certainly face a cash flow interruption. What do you do in the event banks are closed? How will the firm pay the employees? Can you rapidly tap into credit sources? Ideas should be considered that will get the billing employees up and operational as soon as possible to avoid any 'hiccups' in cash flow. Can you relocate to a friend's office? Can you quickly rent an office elsewhere? Is it possible to work remotely and still keep the business afloat? You have the same considerations in the public sector as well. The difference is that profit margins are not the driver, sustainability of services is. Your primary goal is to provide the ongoing services to your customers-the general public.

(c) **Addition and Subtraction Help**. It may sound silly, but remember natural disasters like Katrina and Sandy and then add and subtract

possible problems. As both storms showed us, you may simultaneously lose power for an extended period, lose physical access to your server, lose cell phone communications and lose contact with key people. Take complex scenarios of disaster and then subtract problems to deal with more everyday cases. Katrina was the mother of disasters, but many firms have had to deal with an extended power failure or a server crash. Be sure you can meet the demands of a disaster on every possible level. Don't just stop with natural disasters either. A malware infection on your network can also be a disaster. Recently, malware classified as ransomware is attacking resources around the globe. Specifically, the ransomware CryptoLocker encrypts the data on your computer and any network connected storage. You won't be able to access the data unless you pay a ransom (typically around $300) for the decryption key.

(d) **Test Your Technology** – Since you purchased that high tech backup system and that super expensive media technology, you know the data is on there, right? Have you tested that assumption? These days, backup systems are hard drive based and tape is a thing of the past. Successful backups are still just as important as the old legacy tape drive days. Just because information is being written to a hard disk doesn't mean that it is good data that can ultimately be restored. You must test the restoration process to ensure that the data will be available when needed. Also, it is not uncommon for backup systems to have the ability to create virtual environments. This means that a backup appliance is installed on your local network that backs up in a near real-time mode, typically taking snapshots every 15 minutes. The appliance can also be turned into a temporary resource (normally a server) by using virtualization technology. As an example, if your actual e-mail server failed, you can "spool up" a virtual server that will look just like the failed one very quickly. Some devices will do automatic "mini-restores" on a daily basis to make sure that they can quickly virtualize and get you back in business. If the daily test fails, alerts are sent to the appropriate contacts so that the failure can be addressed. This means that there is a

high degree of confidence you will be able to get back in business as quickly as possible. Needless to say, these backup appliances can be the Holy Grail for business continuity.

(e) **Communication** – We could have put this in the technology section too, but there is a lot more about communication than the technology that is used. We're not just talking about telephone communication either. During a disaster there needs to be a way to communicate with the decision makers. When do you actually "pull the trigger" and begin to walk through the disaster recovery plan that you spent so much time developing? This may mean that you have cell phone numbers for all critical personnel. But what if the tragedy is so severe that the cell communications isn't operable? The experiences of Katrina and Sandy showed how fragile a cellular network can be. Even without a major storm, the cellular network in NYC was crippled by the significant traffic load during 9/11. Perhaps you can't count on cell phones after all. You may need to deploy satellite phones as a backup. Even with satellite phones, you will need some way to keep batteries charged during a disaster. Radio communication may be another alternative if you are close enough and within range. The Internet gives us another alternative if we use VoIP (Voice over Internet Protocol) communication. This could be a simple as a Skype phone call, although you do need a way to get on the Internet to begin with. Perhaps e-mail is your preferred communication method. Again, you will need access to the Internet or those old fashion analog phone lines and a modem to dial in. Just like testing your technology, make sure you periodically test your communication methods.

(f) **Finish Strong** – What good is a disaster recovery plan that is partially completed? Probably just as good as a broken levee. Many firms start strong and then the disaster recovery effort sort of peters out. The planning process can be exhausting, time-consuming and labor intensive. Nonetheless, the process needs to be finished as strongly as it

was started. Make sure that all employees are aware and have reviewed the plan. Test the final plan and publicize the plan so that all know where they can locate it in the event of an emergency.

(g) **Review the plan every year**. Your technology changes, your people change, the nature of threats sometimes change and your business may change. No plan will last forever, and in a world where technology changes so swiftly, an annual review of the disaster recovery plan is time well spent.

Technology Facilitates Recovery

Most firms dread spending money, especially on technology, because technology is expensive. Lawyers will notoriously rub two nickels together until the buffalo screams. It is important for law firms not to be penny wise and pound foolish. It is a very foolish law firm that does not understand how critical the backup system is to the success of a disaster recovery. It must be able to successfully restore data and system files in the event of a system failure data is lost. A data backup is the last line of defense in recovering data after a disaster, so it's critical that a firm implement a backup solution that is both reliable and redundant. A backup schedule must be set according to a firm's needs. How far back does data need to be recoverable - a week, two weeks, a month, six months? The answer to this question will determine how the backup schedule is configured and what technology is best to deploy. Backup data should be available onsite and also sent offsite. The off-site data can be used to re-establish the business should the physical facilities be damaged. A severe weather event, fire, malware infection or bursting water pipes can render your computer systems inoperable. The offsite information will allow you to quickly get back in business.

Recently, with the cost of storage per gigabyte coming down in price, it has become more cost effective to use removable media such as external hard drives as the media of choice, as they are more reliable than tapes and don't have to be cleaned. If the firm or business doesn't have an IT department, support staff play a key part in the backup process, as they are usually the employees who are responsible to swap out the backup media on a nightly or weekly basis. They also

may have the responsibility of storing media offsite if not automatically transmitted via the Internet. This would include switching out any external hard disks that are used for backup purposes. Removable media is more appropriate for small firm operations, where data volume is smaller and there are less impacted individuals. Consider investing in a backup appliance of sufficient size to hold data going back several weeks along with those 15 minute snapshots. It should also have virtualization capability and encrypted offsite storage via the Internet. Implementing a backup appliance does not require that someone swap out media and take data offsite. Any time you can remove a human being from the process the better off you will be.

All important electronic devices such as computers, servers, networking hardware, phone systems, etc. should be kept on Uninterruptible Power Supply (UPS) devices, which are nothing more than “smart” batteries. This will protect equipment from dirty electricity, surges and outages, all of which can cause damage to equipment. A battery backup may be able to supply the phone system with enough power during an outage to allow you to continue business operation or communicate with rescue personnel. These battery backup devices will allow computing equipment the chance to shut down properly, which can help to prevent data loss or corruption of files. Software configurations of all networking devices should be backed up and stored in a secure location. In the event that replacement equipment is needed, restoring the configuration of these devices will bring them online faster than configuring them from scratch.

Contingency plans for hosted services during recovery should be discussed and planned for. How will you communicate with the outside world if you can’t use e-mail or cell phones? The IT personnel can help plan, identify and track potential vendors and providers of these services in the event of a disaster. More vendors are now offering the ability to host virtual servers on which data could be restored in the event that your computing infrastructure is lost. Data and applications could thereby be accessible while waiting for replacement equipment to arrive. Having ‘hot’ outsourced options available is important to getting communication and business channels operating again. Your IT department or support staff can also help to track the locations of technical

service contracts, software licenses, insurance documents and other important documentation that might need to be provided during disaster recovery. Being able to readily locate and retrieve these documents is critical – and often overlooked.

This is a good place to also mention "going to the cloud." We are big fans of what we call a hybrid cloud solution. Your servers and backup appliance are housed at a datacenter, where there is redundant power, cooling and Internet connectivity. Should something happen to your office space, the employees can work from home or any other place that has Internet access to connect back to the datacenter. Most datacenters will also rent out emergency office space if a disaster strikes. In this way you are still in business even if your building is inaccessible or severely damaged.

Security Issues When Planning/Recovering From Disaster

Security continuity should be an element of the disaster recovery and business continuity plan. As a firm starts to get up and running again, security measures to protect your data and systems should be taken. What steps can you take to ensure that the data remains secure and confidential?

First, make sure the computer or server where information is centrally stored is located in a room that locks or in a locked cabinet. Make sure that the key to this lock is not readily available around the office. This will help to control who has physical access to the hardware that the data is stored on. Two-factor authentication is becoming widely used in protecting critical networking and computing equipment. Biometric access is no longer a part of James Bond movies, but rather is making its way into law firm's standard physical security plans. The physical security of the backup media should be a major concern too, especially if you use external hard drives or (heaven forbid) still using tape. Backup media should be stored in a locking fireproof safe in the server room. A backup set should also be kept offsite for redundancy and should be stored in a locked fireproof safe. Please remember to keep the fireproof safe closed at all times or you might be left with melted – and useless – goo. Obviously, securing backup

media does not apply if you are using a backup appliance, which we think is a must-have technology today.

The office space should be protected as well. Fire and security alarms are of the utmost importance. In coordination with security alarms, motion sensors can be used to detect movement. If motion sensors are placed in or near the server room, they can add another layer of protection in the firm's physical security plan.

Physical security is only part of the equation - what is often overlooked is the electronic security that should be implemented and enforced. All electronic data stored on backup media should be encrypted and password protected. Passwords for users, backup media, Administrators, etc. should not be written on a piece of paper and stored in the server room by the equipment. Company laptops should be encrypted to protect data in the event that they are stolen or lost. Laptops are now available that require biometric access in order for the user to log into them. This adds another layer of security to protecting confidential data stored on laptop hard drives, which may be particularly important in the case of a disaster, where laptops may fall into third party hands. Strong user and equipment passwords should be enforced. During recovery, if third-party vendors are used as a 'hot' option to get the business up and running, ensure that any data that is stored or transmitted is encrypted and protected. This information should be laid out in any contract or agreement before it is signed. The security and confidentiality of data and equipment is vital and should be addressed in the disaster recovery plan.

Though Katrina proved to be a vicious lady, she left us all some invaluable lessons for the future. First and foremost, after watching hundreds of law firms close, many of them never to reopen, the legal profession has begun to take disaster recovery seriously, and is willing to spend more time and money preventing a disaster from crippling a firm for an extended period of time.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com