Disaster Planning Tips from the Law Practice Division

by Sharon Nelson and Jim Calloway

With so many recent disasters and perhaps more ahead, the ABA Law Practice Division advises you to do some planning **NOW**.

Have a Disaster Recovery Plan which you review annually. Define who is responsible for what. It should be electronic and in the cloud as well as in paper. Several trusted members of the firm should also keep a paper copy at home.

Communications are always the #1 problem. An emergency contact list should be in paper and in the cloud where it can be accessed via a computer or a phone.

In case of flooding or mass destruction, it is best to have a backup in the cloud. Test your backup regularly to make sure it is working. There are many reputable cloud providers – examples include Mozy, Carbonite, Backblaze, CrashPlan SMB and Acronis.

If you have case management in the cloud (Clio, Rocket Matter, MyCase etc.) you will be back up and running more quickly. If you are using external hard drives or flash drives, they are most safe in a dishwasher if flooding is anticipated. You can carry a waterproof flash drive with you in a waterproof bag for extra protection and mobility.

Office 365, the cloud version of Office, will also help with this.

How will you pay your people? It is advisable to have cash available in a waterproof safe. Banks may not be open for a while. Also in that safe should be any critical documents, such as your insurance policy, articles of incorporation, etc.

In case you lose power, consider a generator. Also, make sure phones and laptops are fully charged, with power banks offering you power reserves. If you have small handheld battery chargers for phones, make sure all of those are charged as well.

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.