DISASTER PLANNING:

It's Not Just for Hurricanes

Are You Ready?

Louisiana State Bar Association

Serving the Public. Serving the Profession.

Would you and your practice survive these common disasters?

Start your disaster planning by taking a few moments to think about your office's ability to survive these common "disaster" scenarios.

- **FIRE/HURRICANES/TORNADOES/NATURAL DISASTERS**: If your office was completely destroyed by fire or natural disaster like a hurricane or tornado, how long would it take you to contact all of your clients, recreate all your computer data, contact your insurance company, process invoices, contact opposing counsel and generally get your practice operational again? Who would be responsible for performing each of these functions?
- **ILLNESS**: If you had a heart attack tonight, or otherwise had to be out of the office unexpectedly or indefinitely, are your files organized so that someone could pick up your caseload without your clients suffering any disadvantage? Could anyone actually find anything on your desk or in your files? Do your answers change if your assistant was out sick or away on vacation at the same time?
    - Conversely, if you have a partner/associate who was suddenly disabled, do you or someone in your office know his/her schedule for the next three months? Do you or someone in your office know the status of all matters in your office?
- **DISABILITY**: If you or a partner in your firm is disabled for an extended period of time, will you be able to draw a salary? If so, how much and for how long? If you are a sole practitioner and the only rainmaker, how will expenses of the firm be paid while you are out and unable to make rain?
- **SUDDEN PERSONNEL CHANGES**: If your secretary/legal assistant/bookkeeper suddenly quit, do you know their filing systems so that you can find information in their desks, in their (or your) files or on their computers? Do you have copies or know where they keep the keys for filing cabinets, etc.? Do you know all their respective passwords (including voice mail, computer login, e-mail, the accounting package and any other software applications they use)?
- **THEFT OR BURGLARY:** If all of the computers in your office were stolen over the weekend, do you have all the serial numbers of the equipment, the original cost of the equipment, the value of the equipment and the ability to recreate all of the data on the computers?
- **MAJOR COMPUTER MALFUNCTION:** If your computer(s) were attacked by a virus and/or your data was rendered unusable or unavailable, would you be able to retrieve your data to start anew?
- **TRUST FUND THEFT**: If one of your staff members disappeared with client trust funds, would you have sufficient records to determine what was taken and when?

If you were unable to answer all of these questions as quickly or as adequately as you would like, then you need to do some disaster recovery planning. Regardless of the size of your firm or practice, you need to create an easy to implement plan that will assist you, or anyone in your office, if an unexpected practice interruption affects you, your staff or your firm.

—*Adapted with permission by Louisiana State Bar Association Practice Management Counsel Shawn L. Holahan from source material,* Managing Practice Interruptions*, published by LawPro;* Disaster Planning: Protecting Your Firm, Your Clients and Your Family*, 2001, by Patricia Yevics, Director, Law Office Management Maryland State Bar Association, Inc;. and* Prepared*, published by the South Carolina Bar Association.*

Table of Contents

Introduction

How prepared are you for a serious interruption to your practice? Accidents or disasters that have the potential to interrupt or destroy a law practice come in many forms—they can be natural, technology-related or man-made, intentional or accidental. Foresight, planning and preparation are critical to minimizing the impact of any accident or disaster and may even prevent a minor event from becoming a major one.

The Louisiana State Bar Association has prepared this series of checklists to help ensure your practice is capable of withstanding a disaster. Although you're unlikely to ever experience a major, practice-ending disaster, the fact is disaster can strike anyone, anywhere, anytime. You may have to deal with a computer crash or loss of data, theft or malicious damage, fire or flood, or the loss of a key lawyer or staff person.

The better prepared you are to respond to one of these events, the faster you will have your firm back up and running, with minimal financial loss or service interruption. To ensure this continuity, you need a plan. That plan starts with a thorough assessment of your exposure, detailing how you will minimize the impact of each exposure on your practice and providing a roadmap for how you will recover.

Once your areas of vulnerability are identified and your response plan is developed:

- Put it in writing and distribute it to all firm employees;
- Keep one copy in the firm disaster recovery file, along with other critical information for responding to a disaster or interruption; and
- Put the second in a secure, off-site location.

By using the checklists and tips in this booklet, you can prepare for unexpected minor and major practice interruptions and thereby protect your employees, your practice and your property.

Create Your Emergency Response Team

Assign an Emergency Response Team (ERT) or person: The ERT or person is responsible for overseeing and coordinating the preparations for and the responses to a disaster or emergency. The ERT or person will provide the required leadership and direction and will make all final decisions. He or she will also have to periodically review and update all disaster recovery plans to take into account any changes in personnel or circumstances. Among the tasks to consider:

1. Designate a member of the firm or Emergency Response Team to be responsible for determining when you are in an emergency and define decision-making authority.
2. Decide how emergency information is to be communicated to employees.
3. Determine who issues the "all clear," when it's issued and how.
4. Identify and train members.
5. Have some employees complete first aid and CPR training.
6. Name alternates in case of absence or unavailability, and appoint new members immediately if there is any turnover.
7. Identify the types of potential dangers that should be reported to, or by, firm employees.
8. Inform other employees about the team's function and who is a member.
9. Schedule an annual date to review the team dynamics and update emergency checklists and procedures.

Create Your Emergency Response Team, con't

Describe routine duties of the ERT: The ERT or person is responsible for making sure office safety needs are met at all times. For example:

1. Regularly look for hazards (overloaded electrical circuits, improper use of extension cords, blocked stairways and exits, etc.).
2. Verify exits are clearly marked.
3. Check for proper lighting, including emergency lighting.
4. Fire safety:
    a. Ensure fire extinguishers are available and charged.
    b. Verify there is a working fire alarm.
    c. Check smoke detectors and/or CO (carbon monoxide) detectors to ensure they are working properly.
    d. Verify that sprinklers function.
5. Stock emergency supplies and first aid kits.
6. Conduct safety training for employees.
    a. Train employees to recognize and report possible emergencies.
    b. Provide each employee with phone numbers for police, fire, building security, etc.
    c. Post emergency phone numbers in prominent locations in the office.
    d. Consider utilizing a fire-resistant and, where appropriate, fire-proof safe.
7. Test door locks and alarm system periodically.
8. Have a staff member in your reception area to greet visitors at all times.
9. Provide cable locks on laptops.
10. Make sure bookshelves are secured with bolts to the wall (to prevent them from tipping).
11. Keep a good stock of emergency supplies (flashlights, a radio, cell phones, batteries, candles, blankets, water, toilet paper and non-perishable food).

Develop a building evacuation plan: One of the chief duties of the ERT or person is to develop or customize a pre-existing building evacuation plan. Every evacuation plan should address the following:

1. Identify escape routes.
2. Identify employees who need help during an evacuation and their location in the office; assign a helper to each, as well as alternative helpers in case of absence.
3. Identify a first aid treatment area and a list of employees certified to administer first aid.
4. Identify "evacuation marshals" who are responsible for making sure everyone is out of your office, and for securing it when they leave.
5. Assign different people to monitor different areas and entrances.
6. Assign alternates in case the primary person is not present.
7. Make sure people who are assigned this task know where keys are located and how to operate magnetic locks, alarms and other building security.
8. Post a sign on your door indicating the firm's closure, and provide a contact number (ideally have this sign prepared beforehand).
9. Establish a check-in procedure at a gathering place away from the building in order to account for everyone.
10. Hold regular emergency evacuation drills.
11. Start with announced drills to get the procedure down, followed by unannounced drills.
12. Establish who is responsible for escorting visitors out.
13. Ensure training emphasizes employee responsibility to comply with directions of emergency workers and designated evacuation marshals.
14. Identify specific items (valuable artwork, key records, etc.) to be evacuated from the office in the event of an emergency. This should happen only if time permits, and without endangering people. Assign responsibility for this task, re-emphasizing human safety over the rescue of objects.

Inventories

A complete disaster recovery plan includes an up-to-date inventory. A detailed inventory of ALL office contents is essential for your disaster recovery plan and insurance purposes. Supplement your inventory with a videotape or photographs of everything in every room of the office. Document items in drawers, filing cabinets, storage areas and closets. This is the only way to make sure you have a complete record of everything, including smaller items.

Create a list of office equipment that includes item description, make, model, serial number, purchase price and date and supplier. Obtain appraisals of any items of significant value. Update your inventory annually or when you purchase anything of significant value. Once this information has been completed, it should be kept off-site. Remember to update the off-site list when you make additions or deletions.

Assign the responsibility for taking a complete inventory to someone in your office, and set a reasonable timetable for completion. (You may want to make this one of the duties of the E.R.T. or E.R.P.) Depending upon the size of your office, this can take anywhere from one week to one month. Once you have made this assignment, mark the date for completion on your calendar and review it on or near that date.

At a minimum, the inventory should include the following information, which should be updated each time a new piece of equipment is added or discarded:

1. Computer hardware equipment, including location, serial number, original price (if known), purchase date (if known) and original vendor (if known).
2. Software, including serial number, original price (if known), purchase date (if known) and original vendor (if known).
3. A printed hard copy list of library contents and subscriptions.
4. Other office equipment, including fax machines, photo copiers, dictation equipment and telephone equipment. Where possible, include serial numbers, original prices, purchase dates and vendors.
5. If you have not done so, make certain that you begin to keep information on purchase date, price and vendor.
6. You should also have information on all maintenance contracts for equipment in your office.
7. When new office furniture is purchased, try to include information about it in your inventory.

Storing Client Files

Your client files contain irreplaceable information. Reconstructing a lost file is a very time-consuming process. In most cases, you will never be able to completely reconstruct everything that was in a lost file. Furthermore, you have an ethical duty to protect your client files.

Take the following steps to protect the contents of your client files in your office:

1. Keep active files up-to-date and well organized. This will help you, or your replacement, locate file information when resources are limited and stress is high.
2. Properly store files and documents. Don't leave your files on desks, chairs, the floor or windowsills. Anything left out is more susceptible to theft, fire, water or smoke damage. They should be placed in a fire-resistant filing cabinet.
3. Take extra precautions with irreplaceable documents. Client originals and other irreplaceable documents should be stored in a fire-proof safe (not a fire-resistant one).
4. Don't put critical documents or files on or near the floor or in basements, if possible. This can help minimize the potential for water damage.
5. Store photographs and negatives separately. Keeping them separate may be a lifesaver in the event one set is damaged or destroyed.

What to Store Off-Site

Closed client files should be stored off-site at a proper storage facility. There are companies that specialize in managing and storing documents, as well as shredding and proper disposal when the time comes. You may also find that having off-site copies of critical, practice-related documents could be helpful if your office is destroyed or can't be accessed. Consider keeping copies of the following documents in a secure, off-site location:

1. Your disaster recovery file and all supporting information (contact lists, etc.);
2. Partnership and other firm-related agreements and documents (including minute book);
3. Leases or sub-leases;
4. Insurance policy and broker information;
5. Inventory list, including videotape or photographs, if taken;
6. Employee contact list; and
7. Any other important administrative records or documents.

Calendar Checklists

Almost all areas of law practice are deadline driven to some degree. Areas such as litigation live and die by deadlines. For this reason, it is critical for lawyers to keep an up-to-date calendar. Take the following steps to protect this information and make it available to others in an emergency:

1. Have a current calendar in at least two different places. This can include at your office and/or at home.
2. Make sure others have access to it. In addition to your own support staff, one or more other staff or lawyers at your firm should have access to your calendar in case both you and your staff are unavailable.

Financial Systems Checklist

Any disruption to a firm's revenue stream, especially a disruption that lasts for some time, can have a significant impact on a firm. As well as the usual ongoing expenses, such as payroll, you may have to finance a myriad of disaster-related costs. To prepare, include the following measures in your plan:

1. Regularly back up all financial and billing programs. This will ensure that you have access to all critical financial information, including accounts payable, accounts receivable, dockets, client work in progress and disbursements and accounts receivables.
2. Store some blank checks in a secure, off-site location. A small supply of company checks helps to communicate that it's "business as usual."
3. Arrange a line of credit. A line of credit can be a lifeline, ensuring cash flow until you can get your billing and collection procedures back in place.

Insurance Checklist

Having adequate insurance in place is one of the best things you can do to prepare for a disaster. Consider all types of insurance, including:

1. Property insurance (if you own your building); contents insurance, including extra riders for computers or other equipment of significant value;
2. Commercial general liability for third-party bodily injury or property damage;
3. Business interruption insurance;
4. Crimes coverage;
5. Disability, life or other appropriate personal coverage;
6. Review and evaluate the adequacy of your coverage, including any policy limits.

Pay particular attention to any stipulations, exclusion clauses and to what extent consequential losses are covered (they most likely are not). Consider if you should get any of the following coverage options:

a. Replacement value;
b. Valuable papers coverage, including cost to recreate files; loss of income;
c. All risks, including floods and earthquake;
d. Cleaning/restoration costs;
e. Payment of interim rent;
f. Sprinkler/water damage; and
g. Personal items (review whether your homeowner's coverage covers these items).

Ensuring you are properly insured is an ongoing process. You should regularly review your circumstances and the adequacy of your coverage, ideally annually. Be conservative in making your estimates, and consult with your broker. Some firms tie a coverage review into the renewal process as a way to ensure this task takes place annually. Review your coverage if you make any significant purchases or if there are any changes of circumstance that warrant coverage changes.

Computer Systems

Protect your investment in your computer systems—and the information stored on them—by doing the following:

1. Identify sources of rental/loaner computer equipment and service people with necessary expertise to support it.
2. Use uninterruptible power supplies (UPS) and surge protectors, especially on servers and phone systems.
3. Use anti-virus software and keep virus definition files up-to-date (at least weekly; this can be set up to happen automatically).
4. Implement appropriate security on your servers and networks.
5. Use firewalls at any external network access points.

It is important to document all new programs, updates, patches, modifications and customizations to computer systems and to store a hard copy of this documentation off site, along with software license numbers, activation codes and copies of any original CDs. You should also have documentation that explains the standard installation and set up of all programs on a standard office PC. This will allow you to recreate one from scratch if necessary or create a prototype for quick restoration.

If you are cloud-dependent, have the cloud-provider contact information readily available.

Computer Back-up Checklist

Computers and other legal technology are a critical part of practicing law. Every law firm has huge amounts of irreplaceable data on server and/or desktop hard drives. The most critical part of any disaster recovery plan is backing up the data on your firm's computers. A back-up will allow you to recover when hard drives are lost or damaged due to theft or fire, or when they fail for whatever reason. Computer hard drives are complex pieces of electronic hardware that have moving parts. All hard drives are subject to failure, and most ultimately will if they are used long enough.

Several back-up options exist. You should familiarize yourself with them and the pros and cons of each. Among the most used back-up options are disk-to-disk back-up, back-up tapes, and cloud service back-up providers. Disk-to-disk back-up refers to copying information to a shared network drive, SAN or NAS or other locally managed disk. Back-up tapes use tape to secure large amounts of business data. While both disk-to-disk and back-up tapes give the attorney complete control over the physical location of the data, data may not be usable or accessible if the disks or tapes were destroyed or if the person with the responsibility of having the disks or tape is not available. Cloud back-up services can back-up data for recovery with infinite storage work in the background (e.g, Dropbox, Backblaze, Mozy, Carbonite and CoreVault). However, because client information is going to a third-party provider, the lawyer must choose a provider with care to ensure that client data is secure and kept confidentially.

Some lawyers rely on USB/thumb/flash drives to back up data. Certainly, using these drives are inexpensive and are better than no back-up. However, be aware of the limitations. These drives can be easily lost due to their small size, and a good one can safely sustain only a certain number of write-and-erase cycles.

Depending on the option that you are using, consider the following things to ensure you have a complete and reliable back-up:

1. Do a full back-up: Full back-ups are preferred to partial back-ups. Having everything that was on your hard drive is better than finding out you need a critical file that isn't in your back-up and is not otherwise available.
2. Do back-ups daily: Modern back-up hardware is able to do complete back-ups of large hard drives in a matter of hours. Back-ups can be set to run automatically, usually in the middle of the night. Doing a daily back-up ensures you are as up-to-date as possible. It will have all of the work and data that you created up until the end of the previous day. If you are using the thumb drive approach, you need to find the discipline to back up every day.
3. Identify responsible person(s) and alternatives: Doing the back-up should be a mandatory responsibility that is assigned to a specific individual and a specific alternate individual. You want to ensure that a back-up is done every day without fail.
4. Review the back-up log: Most back-up software programs create a log report when a back-up is completed. This report details what was backed up and if there were any problems.
5. Regularly do test restores: Don't believe the back-up log. Periodically, it will report successful completion of a back-up, despite the fact that some or all of the data to be backed up was missed. The only way to truly test your back-up is to regularly do a test restore of selected files and folders.
6. Identify an off-site storage location: Tapes, disks and thumb drives left on top of your server in your office will be destroyed or taken along with your server if there is a fire or theft. You should store at least some back-up tapes, disks, thumb drives in one or more safe off-site locations.
7. Rotate and keep generations of tapes: Don't use the same tape over and over; rotate your back-up tapes. For example, use a series of five tapes, one for each night of the week. This can be helpful when database corruption is detected some time after it occurred. Having an older back-up will allow you to reach back to an earlier date if necessary. Some firms keep end-of-week, end-of-month or end-of-year back-ups.
8. Replace tapes regularly: Back-up tapes degrade over time and with use. You should replace your back-up tapes every six months. When they get to the end of their life, rotate them out as the end-of-month tape, etc.
9. Don't forget data on desktops, laptops and other devices: Usually, server back-ups are configured to only back-up data on servers. Make sure that data not on the server (e.g., data on C and other drives not on the server) of desktop computers, laptops and other devices get backed up as well.
10. Have staff back up the phone numbers stored in their cell phones.
11. Make sure open files are being backed up: Some back-up software, and in particular older versions, will not back up files that are in use or "open" by other programs. Central accounting system, e-mail and other database files often remain open 24 hours a day. Make sure that your back-up is getting all open files.
12. Create written instructions for restoring: Many offices have one or two people who know how to do a back-up, but no one who knows how to restore backed up data. Create written instructions and train several people to do this task.
13. Find a hardware back-up buddy: If your back-up server and tape unit are destroyed or stolen, you could find yourself with a good back-up tape and no compatible tape unit to do a restore. Ideally, find someone who has a server and tape unit that is identical to yours.

A partial back-up from last week is better than no back-up at all. If you aren't doing full regular back-ups, at least spend some time backing up some of your important files. It is easy to copy files onto a CD or some type of removable storage device. It is even easier to simply copy them to another computer on the network.

Alternative Communications

Some emergencies will disrupt normal telephone, e-mail and facsimile communication channels. To prepare for this, consider implementing other communication channels:

1. Do you have one or more cell phones that you could use in place of your normal phone?
2. Determine ability/procedure to re-route phone lines to an alternative location/person.
3. Identify where the calls should go and who should be there to answer them.
4. Determine who has the authority and responsibility for implementing the alternative communication system.
5. Set up an emergency communication center and determine how to:
    a. Answer normal incoming calls;
    b. Respond to employee/client/court/etc. questions.
6. Set up a hotline for employees that would provide them with information (either via a live person or a recorded message). Consider whether your employee hotline should allow employees to leave messages.
7. Use your Web site, or an alternate Web site, to provide information and updates to all interested parties.
    a. So you are not doing it in the middle of a crisis, consider creating the site, or a sub-page for your existing site, before the disaster occurs.
    b. Consider whether parts of this site should be secure to provide confidential information to employees or clients.
    c. Consider whether broadcast e-mail capability would be helpful for communicating with employees, clients or others.
8. Are the direct phone lines in your office routed through your phone system server? Sometimes they are not, and if so, may not fail in the event the phone system server does. Can you/should you set this up?

Emergency Contacts

Without current contact lists, your ability to communicate with staff, clients and other concerned parties will be limited, if not impossible. Create contact lists for each of these groups. Update these lists regularly. Key partners and employees, as well as emergency response team members, should have access to these lists at work and at home.

Employee and Client Contact Information:

1. Full name
2. Home and cell phone numbers
3. Spouse/emergency contact information
4. Alternate contact information
5. Home address
6. Name and address of spouse or partner's employer
7. Special medical needs

Emergency Contacts:

1. Emergency-related assistance
2. Active clients
3. Opposing counsel
4. Courts
5. Landlord or property manager
6. Bank/financial institutions
7. Accountant
8. Payroll company
9. Insurance company and broker
10. Suppliers and vendors

Pick a Personal Back-up

All lawyers, and in particular sole practitioners, should reflect on the issue of who would step into their shoes in the event of incapacitation or death. In larger and medium-sized firms, someone else in the same practice area may be available to take over a disabled lawyer's practice.

However, lawyers in small firms may not have someone with the necessary experience or capacity to take over. One possible solution is an "emergency buddy"—a qualified peer who can help notify clients, take on your caseload and run your practice in case of personal emergency or other disasters. Consider making this a reciprocal arrangement: you each agree to step into each other's shoes. It may make sense to arrange for your files to go to two or more lawyers. Consider an agreement to close law practice, limited power of attorney and sample will provisions.

If your buddy is at another firm, be aware of and follow the applicable ethical requirements regarding conflicts, advance client consent, etc. Regularly provide your buddy with any updated information necessary to carry out his/her role. Make sure your staff is aware of your plans, as they may be inclined to send your files to someone else. You can adapt and follow the procedures outlined in this booklet, to the extent applicable, based on your staffing, location, etc.

Back-Up Office

A fire or a major natural disaster could completely destroy your office or prevent you from accessing it. To plan for this eventuality, identify a possible temporary office space or "hot site."

If you are in a major urban center or want to take extra precautions, consider looking for space away from your immediate area so that you don't find yourself in a situation where a large disaster prevents you from getting to both your main and alternate offices. Larger law firms may need to set up an alternative office that can function as a new central hub for main office functions. Small firms and sole practitioners could plan to work out of someone's home, in space at another office or, if need be, any vacant building.

Remember, recreating a destroyed office involves more than the simple restoration of your back-up data.

1. Determine how work will be assigned, who will do it and how supervision will occur.
2. Identify what tasks or functions could be performed via telecommuting, and identify employees who are suitable and equipped to telecommute.
3. Many law firms already have their lawyers set up to work remotely from home. Consider whether this is an option and, if so, make sure home computers have all standard office software on them.

Equipment that you will need to set up an office at an alternate location:

1. Computers;
2. Telephone systems, printers, facsimile machines, scanner;
3. Network hardware, etc.;
4. Consider taking older, unused equipment to your off-site or home office;
5. Identify sources of rental or loaner equipment and service people with the necessary expertise to support it; and
6. Store a limited amount of basic office supplies at home or at your off-site location as well.

Putting Your Own House in Order

Putting your personal house in order could help you and/or your partners deal with a firm emergency. In any emergency, quick access to certain pieces of personal information is essential.

Prepare a list with the following critical personal information (if applicable):

1. Name, address, passport, insurance card and social security numbers of you and your spouse or partner.
2. All of your and your spouse's or partner's phone numbers (home, work, cell, pager, personal fax, vacation home, etc.) and e-mail addresses.
3. Driver's license and vehicle insurance information.
4. Name, phone number and address of one or more emergency contacts; other special contact numbers (e.g., daycare for your children).
5. Name, address and all phone numbers of your direct employees.
6. Names, addresses and phone numbers of your personal representative, lawyer, accountant, physician and landlord.
7. Location of your will, power of attorney and/or trust agreement.
8. Names, addresses, phone numbers, policy numbers and contact persons for all insurance policies.
9. Location, box number and where to locate key to safe deposit box(es); list of contents of safe deposit boxes and signatory information.
10. Name, address, phone numbers, account numbers and signatory information on all business financial accounts.

You and other key partners or employees in your office should have this information at your fingertips, including at your respective homes.

Make a copy of everything in your wallet, store this information in one or more safe locations that you or someone else can access. Include 1-800 numbers for reporting lost credit cards. This will save you much time if you need this information.

Emergency Response

During any emergency, human life and safety come first. Now is the time for the Emergency Response Team to act, starting with the preplanned evacuation plan.

1. Evacuate, contact and account for all people in your office.
2. Obtain emergency medical attention for anyone who requires it.
3. Mobilize your emergency response person/team: bring together the people who have been charged with responding to an emergency.
4. Once you are certain that your staff is safe, implement your disaster recovery plan and respond to the specific circumstances of the emergency.
5. Make any necessary reports to the appropriate authorities.
6. Review and start to execute the plans in the disaster recovery file.
7. Put the people and resources in place to start the recovery process.
8. If time and safety permit, rescue any identified critical records and valuable property.
9. Make the maximum withdrawal from an ATM. This will give you some cash in case banking or ATM services are unavailable for a short period of time.

The Recovery Process

The recovery process starts as soon as the emergency ends. Implement the appropriate steps outlined in your plan for managing disasters and/or business interruptions.

1. Access and review your disaster recovery file to determine the appropriate next steps and to ensure you have access to all of the required information.
2. Attend to less critical physical and emotional needs of employees. Implement any assistance provided through benefits plans, counseling services or EAPs (Employee Assistance Plans).
3. Mobilize the damage assessment person/team.

   a. Initiate immediate actions necessary to protect and preserve property and records and to eliminate ongoing hazards.

   b. Determine salvage and recovery requirements and time frames; notify insurance carriers as they may provide direction and resources for the salvage efforts.
4. Contact all employees in the instance of an after-hours emergency and employees who were absent from work during a work-hours emergency, and confirm procedures to provide interim status updates.
5. In case of a natural disaster, contact the local emergency operations center to get directions and status information.
6. Implement an Emergency Communications Center: start re-routing phone lines, identify an alternate Web site, etc.
7. Review your insurance policies, and contact appropriate brokers and insurers.
8. Begin the notification process (clients, courts, opposing counsel, post office, vendors and suppliers, etc.).
9. Review calendars to identify tasks that have upcoming deadlines and assign tasks to an appropriate person.
10. Initiate a search for, and transition to, temporary space if this is necessary; begin outsourcing for furniture, equipment and supplies.
11. Help set up employees who will be working from home.
12. Implement other aspects of the disaster recovery plan as applicable.

For insurance purposes, you should carefully document all work done and expenses incurred on disaster recovery-related tasks. Make detailed dockets of all time spent, both billable and non-billable.

Expect the unexpected. There will always be something you didn't plan for or expect. Don't be afraid to ask for help. In a serious emergency, even your opponents may be your lifeline. Offer help to others if possible. They may be worse off than you.

After the emergency is over, and when the recovery is well underway, you should hold a debriefing for your staff. Bring everyone together and thank them for their responses and their understanding of any ongoing inconveniences. Respond to their concerns and provide as much information as possible about the status of the situation and future plans. Seek input from everyone about what worked well and what didn't. Respond and address any new issues raised, and obtain any additional resources suggested in the debriefing.

Again, assemble your entire staff and thank them for their responses and understanding. Celebrate the creativity and caring that occurred in the face of disaster. This is important for the healing process. It may take some employees a long time to put the disaster behind them.

Revisit your disaster plan, using the experience to improve your plan.

CHECKLIST

Create Your Emergency Response Team (ERT)

Assign an ERT/person

- ❑ Assign an Emergency Response Team/person
- ❑ Decide how emergency information is to be communicated to employees
- ❑ Decide how emergency information is to be communicated to employees
- ❑ Determine who issues the "all clear," when it's issued and how
- ❑ Identify and train members
- ❑ Have some employees complete first aid and CPR training
- ❑ Name alternates in case of absence or unavailability, and appoint new members immediately if there is any turnover
- ❑ Identify the types of potential dangers that should be reported to, or by, firm employees
- ❑ Inform other employees about the team's function and who is a member
- ❑ Schedule an annual date to review the team dynamics and update emergency checklists and procedures

Describe routine duties of the ERT

- ❑ Regularly look for hazards (overloaded electrical circuits, improper use of extension cords, blocked stairways and exits, etc.)
- ❑ Verify exits are clearly marked
- ❑ Check for proper lighting, including emergency lighting
- ❑ Ensure fire extinguishers are available and charged
- ❑ Verify there is a working fire alarm
- ❑ Check smoke detectors and/or CO (carbon monoxide) detectors to ensure they are working properly
- ❑ Verify that sprinklers function
- ❑ Stock emergency supplies and first aid kits
- ❑ Conduct safety training for employees
- ❑ Train employees to recognize and report possible emergencies
- ❑ Provide each employee with phone numbers for police, fire, building security, etc.
- ❑ Post emergency phone numbers in prominent locations in the office
- ❑ Consider utilizing a fire-resistant and, where appropriate, fire-proof safe
- ❑ Test door locks and alarm system periodically
- ❑ Have a staff member in your reception area to greet visitors at all times
- ❑ Provide cable locks on laptops
- ❑ Make sure bookshelves are secured with bolts to the wall (to prevent them from tipping)
- ❑ Keep a good stock of emergency supplies (flashlights, a radio, cell phones, batteries, candles, blankets, water, toilet paper and non-perishable food)

Develop a building evacuation plan

- ❑ Identify escape routes
- ❑ Identify employees who need help during an evacuation and their location in the office; assign a helper to each, as well as alternative helpers in case of absence
- ❑ Identify a first aid treatment area and a list of employees certified to administer first aid
- ❑ Identify "evacuation marshals" who are responsible for making sure everyone is out of your office, and for securing it when they leave
- ❑ Assign different people to monitor different areas and entrances
- ❑ Assign alternates in case the primary person is not present
- ❑ Make sure people who are assigned this task know where keys are located and how to operate magnetic locks, alarms and other building security
- ❑ Post a sign on your door indicating the firm's closure, and provide a contact number (ideally have this sign prepared beforehand)
- ❑ Establish a check-in procedure at a gathering place away from the building in order to account for everyone
- ❑ Hold regular emergency evacuation drills
- ❑ Start with announced drills to get the procedure down, followed by unannounced drills
- ❑ Establish who is responsible for escorting visitors out
- ❑ Ensure training emphasizes employee responsibility to comply with directions of emergency workers and designated evacuation marshals
- ❑ Identify specific items (valuable artwork, key records, etc.) to be evacuated from the office in the event of an emergency. This should happen only if time permits, and without endangering people. Assign responsibility for this task, re-emphasizing human safety over the rescue of objects.

Inventories

- ❑ Assign responsibility for taking complete inventory to someone in office to update inventory yearly
- ❑ Create list of office equipment, including description, make, model, serial number, purchase price, purchase date, supplier
- ❑ Obtain appraisals of any items of significant value
- ❑ Supplement inventory with videotape or photographs of every room of the office

Inventory should include, at minimum:

- ❑ Computer hardware equipment, including location, serial number, original price, purchase date, and vendor
- ❑ Software, including serial number, original price, purchase date, and vendor
- ❑ Printed hard copy list of library contents and subscriptions
- ❑ Other office equipment, including fax machines, photo copiers, dictation equipment, telephone equipment
- ❑ Maintenance contracts for equipment in your office

Storing Client Files

- ❑ Keep active files up-to-date and organized in a fire-resistant filing cabinet
- ❑ Keep irreplaceable documents stored in a fire-proof safe
- ❑ Don't store critical documents/files near the floor or in basements to minimize potential water damage
- ❑ Store photographs and negatives separately.
- ❑ Store closed client files off-site at proper storage facility
- ❑ Store disaster recovery files and all supporting information off-site
- ❑ Store partnership and other firm-related agreements, minute book, and documents off-site
- ❑ Store leases off-site
- ❑ Store insurance policy and broker information off-site
- ❑ Store inventory list, with photos or videotape, off-site
- ❑ Store employee contact list off-site
- ❑ Store any other important administrative records or documents off-site

Calendar

- ❑ Keep current calendar in at least two different places
- ❑ Grant access to calendar to others

Financial Systems

- ❑ Regularly back-up all financial and billing programs
- ❑ Store blank checks in secure, off-site location
- ❑ Arrange a line of credit

Insurance

- ❑ Reguarly review your insurance, making sure it is up-to-date and adequate

Computer Systems

- ❑ Identify possible sources of rental/loaner computer equipment and service people to support it
- ❑ Use uninterruptible power supplies (UPS) and surge protectors, especially on servers and phone systems
- ❑ Use anti-virus software and keep virus definition files up-to-date weekly
- ❑ Implement appropriate security on your servers and networks
- ❑ Use firewalls at any external network access points
- ❑ Reguarly document all new programs, updates, etc., to computer systems
- ❑ Store hard copy of documentation, software license numbers, activation codes and copies of original software CDs off-site
- ❑ If cloud-dependent, have cloud-provider contact information readily available
- ❑ Identify person responsible for daily computer back-up
- ❑ Identify alternate person responsible for daily computer back-up
- ❑ Create written instructions for restoring back-up data
- ❑ Regularly review back-up log report for any problems
- ❑ Regularly do test restore of back-up, to make sure all information is successfully backedup
- ❑ Identify and use off-site storage location
- ❑ Identify a "hardware back-up buddy" (someone who uses a compatible/ identical back-up system)
- ❑ Replace back-up tapes regularly
- ❑ Have staff backup phone numbers stored in cell phones
- ❑ Check to make sure any date on laptops, desktops and other devices is stored on server
- ❑ Check to make sure open files are included in the back-up

Alternative Communications

- ❑ Assign responsibility for implementing alternative communication system
- ❑ Identify where calls should go and who will answer them
- ❑ Setup emergency communication center to answer normal incoming calls and to respond to employee/client/court questions
- ❑ Setup employee "hotline" to provide employees with information
- ❑ Setup an emergency sub-page for your website to provide information updates
- ❑ Identify if the direct phone lines in your office are routed through phone system server

Emergency Contacts

- ❑ Create emergency contact list of employees, make sure key partner and the ERT team have access to these numbers at work and at home
  - ❑ Include full name
  - ❑ Include home and cell phone numbers
  - ❑ Include spouse/emergency contact information
  - ❑ Include alternate contact information
  - ❑ Include home address
  - ❑ Include name and address of spouse or partner's employer
  - ❑ Include special medical needs
  - ❑ Create list of contacts that could be useful during an emergency
  - ❑ Include active clients
  - ❑ Include opposing counsel
  - ❑ Include court contact information
  - ❑ Include landlord or property manager
  - ❑ Include bank, any financial institutions and accountant
  - ❑ Include payroll company
  - ❑ Include insurance company
  - ❑ Include computer cloud provider contact information (if applicable)
  - ❑ Include other suppliers and vendors

Back-Up Office

- ❑ Determine how work will be assigned and how supervision will occur
- ❑ Identify employees who can telecommute for certain tasks or functions
- ❑ Setup office software on home computer for remote work
- ❑ Identify equipment that might be needed at an alternate location, and potential sources of rental or loaner equipment
- ❑ Store a limited amount of basic office supplies at your off-site location
- ❑ Consider storing older, unused equipment at your off-site location for use

Personal Information

- ❑ Prepare list with critical personal information
- ❑ Share list of critical personal information with key partner or employee
- ❑ Make a photocopy of everything in your wallet and store photocopies at your off-site location (make sure to copy back sides of cards and include 1-800 numbers for reporting lost credit cards)

Emergency Response

- ❑ Human life and safety come first
- ❑ Start preplanned evacuation plan
- ❑ Evacuate, contact and account for all people in your office
- ❑ Obtain emergency medical attention for anyone that needs it
- ❑ Mobilize your ERT
- ❑ Make necessary reports to appropriate authorities
- ❑ Review and execute the plans in the disaster recovery file
- ❑ Put people and resources in place
- ❑ Rescue any identified critical records/property, if time and safety permit
- ❑ Make maximum withdrawal from ATM