MSBA YLS Disaster Relief Committee

Disaster Relief Plan: Preparing for and Rebuilding Your Practice after a Disaster

---

Version 1.0
June 2008

Updated
Version 2.0
May 2015

Creating a Disaster Relief Plan

Is your office prepared if it were damaged or destroyed by fire, flood or another disaster? How would your law firm deal with the death of one of its attorneys? A plan to minimize the impact of events such as these should be in place at every law firm. The following program provides guidance to law firms to avoid business interruption and loss in the wake of catastrophic events.

A successful disaster relief plan ("DRP") must be written and distributed to all employees of the firm. The content and scope of the plan will vary from law firm to law firm based on a variety of factors. These factors include the number of employees, the location of the law firm, and types of anticipated disasters that may affect the firm. The following should be considered for the DRP:

- Method of communications and several alternative method of communication for lawyers and staff to contact each other in the event of a disaster. Both a calling plan, which designates who will call whom, and methods of communications should be outlined in the DRP.
- Disaster Relief Team – assign a Disaster Relief Team ("DRT") to keep the DRP updated and to initiate the DRP in the event of a disaster. The DRT should include representatives from all functional areas of the law firm, including partners, associates, paralegals, and support staff.
- Procedure for storage of vital information, including computer software, paper files, computer files, and other information or technology. Further, a successful DRP will also contain a procedure whereby all of the firm's electronic information will be stored in a separate location and not in the firm.
- Develop a building evacuation plan, including a location to meet upon the evacuation of all employees and an individual (or individuals) in charge to ensure all employees are present upon evacuation.

Post-disaster checklist should be developed to use to coordinate communication and outreach. The information should include the employee's name, contact information, and the names and contact information for their next of kin. Further, names and contact information of the law firm's clients and vendors should be included on the list.

- Keep insurance policies in a safe location, possibly offsite, and routinely evaluate the coverage to ensure it satisfies your firm's needs.
- Contact legal colleagues and other potential businesses, before a disaster, to determine whether temporary work space can be provided in the event that your office is destroyed or if work cannot be performed at your office.

Further, consider holding a seminar for your employees to discuss the DRP; however, training should be practical. Any fire or other drills should ensure that the employees know where to go and what to do in the event of a disaster. The time of the training should be held periodically to ensure all employees, even newly hired employees, know the firm's DRP.

Averting Disaster With Internet Backup Protocol

Reasons to Use Internet Backup

- Massive crisis events can cause damage to equipment
  - 9/11 Terrorist Attacks
  - Earthquakes
  - Hurricanes
  - Floods
- Other events can cause damage to equipment
  - Equipment theft
  - Fires
  - Attacks by hackers can be easier
- Ways that traditional backup systems fail
  - The systems fail to record information onto the backup media — usually tapes, but also CDs, DVDs and hard drives.
  - People fail to rotate media to and from the backup device or to and from an offsite location.
  - The media is destroyed, stolen, or lost either onsite or offsite or both

Case Study Regarding Internet Encryption Systems

- In 2003, the United States government adopted the Advanced Encryption Standard (AES) as a standard for classified data. It is difficult to comprehend the immensity of this encryption technology's strength. To crack it would take 10 trillion years using a billion computers each of which is 200 billion times faster than today's computers.

Internet Backup

- Questions to ask/Factors to determine
  - How much space will you need?
    - Right click the folder where you save your documents
    - Select "Properties"
    - Look at size line item. 1 Gigabyte (GB) = 1,000 Megabytes (MB)
  - Privacy of your data
    - Is the firm the only entity allowed to view data?
    - Can a third-party access data?
  - Suggested third-party companies
    - Connected Data Protector
    - iBackup Professional and iBackup for Windows
    - Data Protection Services
  - Do-It-Yourself Internet Back-Up
    - First, you need an encryption software
      - SyncBack from 2BrightSparks (free version) or SyncBack SE (pay for version) are recommended to encrypt documents.
    - Second, you need an internet storage service, such as
      - Streamload, Inc.
      - Gmail Drive
  - With an Internet Backup system, you will be able to access documents from anywhere.

5 Steps to Creating Your Disaster Relief Plan ("DRP")

Summary of the Five Critical Steps in Creating a DRP

***Visit http://www.ready.gov/business**

- Program Management
  - Organize, develop and administer your DRP
  - Identify regulations that establish minimum requirements for your DRP
- Planning
  - Gather information about hazards and assess risks
  - Conduct a business impact analysis (BIA)
  - Examine ways to prevent hazards and reduce risks
- Implementation: Write a DRP that address:
  - Resource management
  - Emergency response
  - Crisis communications
  - Business continuity
  - Information technology
  - Employee assistance
  - Incident management
  - Training
- Testing and Exercises
  - Test and evaluate your plan
  - Define different types of exercises
  - Learn how to conduct exercises
  - Use exercise results to evaluate the effectiveness of the plan
- Program Improvement
  - Identify when the preparedness program needs to be reviewed
  - Discover methods to evaluate the preparedness program
  - Utilize the review to make necessary changes and plan improvements

Program Management

- Prepare a DRP Policy
  - Policy should be consistent with mission and vision of law firm
  - Policy should be disseminated
  - Policy should identify employees responsible for developing and updating DRP.
  - DRP Policy should emphasize these goals:
    - Keeping people safe, and developing plan for persons with disabilities.
    - Minimize business interruptions.
    - Protect information, assets, and facilities.
- DRP Committee
  - DRP Coordinator should be chosen to develop program and communicate the program to employees
- Program Administration
  - DRP should be reviewed periodically

Planning

- Should utilize all hazards approach
- Hazards and threats should identified and classified, possibly as:
  - Probable vs. improbable, and
  - Type of damage caused, i.e.:
    - Personal injury
    - Property damage
    - Business disruption
    - Environmental impacts
- Vulnerabilities should be assessed
- Potential impacts should be analyzed

Implementation

Includes identifying and assessing resources, writing plans, developing a system to manage incidents and training employees so they can execute plans.

- **Resource Management**: Resources needed for responding to emergencies, continuing business operations and communicating during and after an incident should be identified and assessed.
- **Emergency Response Plan**: Plans to protect people, property and the environment should be developed. Plans should include evacuation, sheltering in place and lockdown as well as plans for other types of threats identified during the risk assessment.
- **Crisis Communications Plan**: A plan should be established to communicate with employees, customers, the news media and stakeholders.
- **Business Continuity Plan**: A business continuity plan that includes recovery strategies to overcome the disruption of business should be developed.
- **Information Technology Plan**: A plan to recover computer hardware, connectivity and electronic data to support critical business processes should be developed.
- **Employee Assistance & Support**: The business preparedness plan should encourage employees and their families to develop family preparedness plans. Plans should also be developed to support the needs of employees following an incident.
- **Incident Management**: An incident management system is needed to define responsibilities and coordinate activities before, during and following an incident.
- **Training**: Persons with a defined role in the preparedness program should be trained to do their assigned tasks. All employees should be trained so they can take appropriate protective actions during an emergency.

Testing and Exercises

- Benefits of Testing and Exercises
  - Train personnel; clarify roles and responsibilities
  - Reinforce knowledge of procedures, facilities, systems and equipment
  - Improve individual performance as well as organizational coordination and communications
  - Evaluate policies, plans, procedures and the knowledge and skills of team members
  - Reveal weaknesses and resource gaps
  - Comply with local laws, codes and regulations
  - Gain recognition for the emergency management and business continuity program
  - For possible exercises please visit http:// http://www.ready.gov/business/testing/exercises

Program Improvement

- Benefits of Testing and Exercises
  - Train personnel; clarify roles and responsibilities
  - Reinforce knowledge of procedures, facilities, systems and equipment
  - Improve individual performance as well as organizational coordination and communications

Recovering and Rebuilding Your Practice – A Checklist

Damage Assessment

- Secure and stabilize the situation
  - Turn off all utilities
  - Pump out standing water
  - Replace doors and windows
  - Install barriers to keep unauthorized persons out
  - If possible reactivate alarm system
- Evaluate damage to equipment, critical documents and client files
  - Begin recovery process immediately
  - Determine salvageable items
- Document the Damage
  - Photograph the damage
  - Videotape the damage

- Contact your insurer

- Contact building owner/management
  - Determine steps to limit damage
  - Get approval to begin salvage operations
- Contact E&O carrier to inform of disaster; degree of damage and potential impact on client services

- Contact local emergency operations centers
  - Register claims for relief for business continuation

  - Contracts/Agreements
  - Settlements
  - Corporate records
  - Docket and calendar records
  - Pleading files and court papers
  - Current address of client's counsel and contacts
  - Correspondence

- Recover Firm Documents

- Bank's copies of checks and deposit slips and bank statements
- Individual client ledger transactions records
- Client's checking account transactions
- Bank tracking deposited checks back to the account from which they were withdrawn to identify the client/matter

Be sure your payroll service will not be interrupted and that the service has your temporary address for the delivery of checks

Office Operations

- Telephone
  - Use cell phones for communication until temporary service is obtained
  - Arrange temporary service with local telephone company at temporary location
  - Arrange to have phone calls forwarded to new number; or
  - Arrange for a telephone answering service with a prepared message to answer the old number until new system is in place.
  - Arrange for fax and internet use.
- Mail/Courier Services (www.usps.com)
  - If disaster is widespread, affecting postal service as well, check to see that anything mailed with a required deadline was/is received on time.
  - Notify other courts and counsel of damage to postal service and obtain an extension of deadlines due to circumstances
  - Contact postal office and courier services of new, temporary address.

- Equipment
  - Contact equipment vendors re: existing leases/contracts and your/their performance obligations under the terms of lease or contract.
- Identify portable computers/home computers that might be pulled back from home use during recovery period. Assess Damage to Documents
  - Extent of damage
  - Recovery – internally or will recovery services be required?
  - Cost benefit of recovery
  - What stabilization techniques are going to be necessary?
  - What and how much personnel will be required to recover and restore documents?

- Client-Related Documents to recover:
  - All original documents

Recovery Site

- Locate a temporary recovery site/office
  - Secure critical equipment and systems
  - Re-established services

IT Recovery

- To provide the best chance of recovery of hard drives and removable media, follow these tips:
  - Never assume that data is unrecoverable, no matter what it has been through.
  - Do not attempt to power up visibly damaged devices.
  - Do not shake, disassemble or attempt to clean any hard drive or server that has been damaged.
  - Do not use common software utility programs on broken or water-damaged devices.
    - When preparing devices to be sent to the manufacturer or to a recovery service: Package them in a box that has sufficient room for the device and packaging.
    - Place wet media in a container that will keep the shipping packaging from getting wet.

- Acquire additional server(s) with enough capacity to run your applications.
  - Back-up servers at a geographically separate location (mirror data centers/servers).
  - Personnel available and mobile to install and manage server operations at a remote site
  - Back-ups of server configurations
  - Data and application changes backed up

- Obtain network map to begin reconstructing the network.

Communication

- Contact all firm personnel to inform them of the firm's status
  - Degree of damage
  - Location of recovery office
  - Timeframe for recovery efforts

- Get the firm's client list and opposing counsel information. If this information is not available, recreate this information:
  - Write down the names of all of the clients you can remember
  - Have your staff write down the names of all of the clients they can remember
  - Log phone calls from clients and add them to the list
  - Look at ABA, state and local bar sites for attorney-client message boards
  - Place ads in local newspapers letting the public know where your office's contact information
  - Provide contact information on your firm's web site.

- Access recent e-mail from your ISP As client information becomes available, communicate with Clients, Courts and Other Counsel. Inform all parties of the incident, the degree of damage, its impact on operations; provide contact information and the address of the recovery site and/or temporary office.

- Retrieve the firm's docket and calendar information. If the information is not accessible, recreate the list by using some or all of the following tips:
  - Start a fresh calendar, filling in important dates as they become known.
  - Obtain copies of correspondence from clients to find deadlines and dates
  - If available, review court dockets
  - Obtain dates from opposing counsel
  - If your ISP provider maintains e-mails for a specific period of time, get access to those to find dates and deadlines

- Upon retrieval and review of the firm's docket and calendar information:
  - Contact courts and other counsel to reschedule meetings, hearings, court appearances if needed
  - Give clients a status report of any immediate critical dates/deadlines for meetings, hearings, etc. and whether those will go forward or be postponed.
  - Assure clients of the firm's ability to be up and operational quickly.

- After alternative work space has been secured:
  - Provide clients, courts and other counsel new contact information and temporary office location
  - Contact mail and courier services to re-direct mail to the temporary office location
  - Contact vendors with new contact and temporary office location

- Contact your webmaster to set up a disaster status page and direct clients to your site for updated information.

Insurance

- Review business insurance, computer equipment, valuable papers policy language; talk with representative about coverage. Topics to discuss include:
  - Loss of income/extra expense and business interruption coverage
  - Discuss how to record and submit expense information for reimbursement
  - Understand how "loss of income" coverage is calculated

- Set up disaster account codes to distinguish disaster purchases and expenses from normal operating expenses.

Financial Matters

- Contact banks to request replacement checks and deposit books; copies of prior bank statements and other records, if needed.

- Determine any short-term cash flow needs that might be needed and discuss/arrange with insurance company/bank. Sources for short-term financial assistance:
  - Short-term, unsecured loans (FDIC)
  - SBA
  - FEMA
  - Disaster unemployment assistance
  - Disaster Relief Funds

- Recover trust account transactions from: