



Summer 2003

Law Firm Disaster Plans: Preparing for the Unthinkable

Since Sept. 11, law firms across the country have come to recognize the importance of having a comprehensive disaster plan in place. These plans should be reviewed regularly to assess their validity in light of external and internal developments and to ensure that they continue to effectively address a number of critical areas, including the protection of documents, computers, and data, insurance, and staff security.

Insurance Coverage

While the appropriate policies and coverage will vary, those that law firms should consider include:

- All-risk building property damage
- Business interruption
- Extra expense
- Valuable papers
- Accounts receivable

Some of these may be included in existing policies, but others may require separate riders or endorsements. Check with your insurance broker or agent about terrorism coverage, as well.

Records, Data, and Computers

To minimize the effects of a disaster, law firms should maintain off-site copies of the following (depending on where the off-site copies are kept, a second set of off-site copies might be kept at another location in case the backup can't be retrieved from the first):

- Current calendar/docket
- Current addresses of clients, counsel, and other contacts
- Current client and matter lists
- Vital client records
- Billable time and receivables information (both historical and current)
- Leases
- Partnership agreements
- Inventory of physical assets
- Insurance records

Despite the reluctance of some attorneys to shift to paperless files, it's worth noting that electronic data are significantly easier to store and replace than paper.

Firms should take a number of additional measures to protect computer files and data. Emergency shutdown procedures should be established, and arrangements should be made for emergency access to a backup computer(s) through a vendor or other source. Regular backup tapes should be made and stored off-site.

Protecting computer operations will be critical to a prompt recovery from disaster. The disaster plan should account for systems failures by providing for:

- Recovery from processing interruptions
- Continuation of processing in the absence of key personnel
- Backup files of application programs
- Regular testing of error recovery procedures following short-term failures
- Rotation of computer operations and programming duties among staff

Current copies of all operating systems, source and object programs, and master files should be kept off-site. Verify that all vendors offer sufficient technical support and maintain an adequate inventory of necessary replacement parts.

Staff Security

The evacuation plan is probably the most important measure for staff protection. An evacuation route should be mapped, and all employees should be required to complete at least one test run. Establish a meeting place so head-counts can be taken.

A Web site and toll-free phone number should also be established so employees can check in. Maintain alternative contact information (e.g., cell phone numbers or home e-mail addresses) for all staff. The plan should also provide a method to transport employees home or to an alternative work site.

Finally, depending on location, consideration should also be given to having enough food and water on hand in case people cannot leave the building for several days.



623 State Street
Meadville, PA 16335
814-724-5890
meadville@mpbcpa.com

[Back To Index](#)
[Home](#)

The articles in this newsletter are general in nature and are not a substitute for accounting, legal, or other professional services. We assume no liability for the reader's reliance on this information. Before implementing any of the ideas contained in this publication, consult a professional advisor to determine whether they apply to your unique circumstances.

© 2003