

# Emergency Preparedness Pointers for Lawyers

By Paul Sullivan

**D**an Quayle is quoted as having said, "We are ready for an unforeseen event that may or may not occur." Although this line is repeated to poke fun at the former veep, it's not without wisdom. Preparing for an unforeseen event that may or may not occur can be frustrating and time consuming, but failing to prepare can be catastrophic both to you and your business.

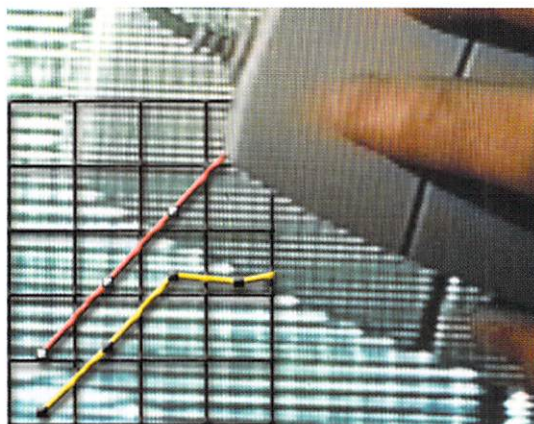
Previous articles in this space have addressed computer failure and loss of key employees – how to prepare for such events and how to recover from them. This article addresses the more widely accepted understanding of a disaster: the catastrophic loss of facilities and/or contents, interruption of services, and other extraordinary events that cause distress to the firm.

When a disaster occurs, your first and most important order of business is to provide for the safety of your employees. The second task is to get operations back to normal as quickly as possible. Both require specific plans.

## Emergency action plan

OSHA requires that every business have an emergency action plan. If you have more than 10 employees you are required to have it in writing; otherwise, you can communicate it orally to them. The plan identifies escape procedures and escape routes. It designates specific employees to perform specific tasks, and it outlines procedures to account for all employees. It also sets out the preferred means of reporting fires and other emergencies. Having the plan is just one component, though. It's also important to keep the plan updated and perform training and drills.

Here's a checklist of the important features of an emergency action plan.



*Let's face it – sometimes you can't prevent fires, floods, violent attacks and the like from wreaking havoc in the workplace. But you can prepare for the worst.*

1. Designate a responsible person to prepare the plan, coordinate it with others in the office and review it periodically.
2. Determine whether to evacuate or take an alternative approach for specific incidents.
3. Designate exit routes for each part of the office.
4. Designate an assembly area.
5. Assign designated individuals the job of accounting for employees.
6. Assign someone the task of reporting emergencies.
7. Establish a training program (specific training for emergencies, alternate optional training in First Aid, CPR, etc.).

## Disaster recovery plan

The disaster recovery plan is a guide to recovering from the effects of a disaster.

Before designing the plan, however, do a risk analysis. A risk analysis begins by identifying every possible event that can affect your business – fire, flood, tornado, vandalism, loss of power, loss of telephones, loss of critical systems, medical emergency, bomb scare, violent intruder, etc. Once you identify the possibilities, consider the probabilities – how likely is the event to occur? Also consider how much advance warning you may have, how long the event will affect you, and what parts of your business will be affected. Once you have an understanding of the potential impact, you can design a plan accordingly.

The primary goal of a disaster recovery plan is to keep the office running. If you plan for the worst-case scenario, you can then easily adapt to meet a less demanding recovery need. Here are some questions to ask before a disaster strikes.

1. How long will it take to get replacement equipment, particularly computers and phones?
2. Is there an up-to-date list of the computer hardware and its configuration?
3. Is the original systems software with patches readily available for your new equipment?
4. Are backups of data good? Are you sure – i.e., do you test occasionally to guarantee the integrity of your data?
5. Is application software with the most current updates readily available?
6. What are your options for alternate space?
7. Do you have a list of client names and addresses so they can be notified of your situation?
8. Do you have a list of vendor names and addresses so they can be notified?
9. For the foregoing questions, is the

## More on disaster recovery

Come to the Law Office Economics Section's breakfast symposium at the ISBA Annual Meeting in Lake Geneva on Friday morning, June 21, and get a disaster-recovery manual loaded with great information. Watch the *ISBA Bar News* and Web site for registration information.

information in a secure location and readily retrievable?

10. What about records recovery? Which records cannot be replaced? Which can?

11. Are you adequately insured for all types of potential interruptions?

Two of the many resources available to help you develop a disaster recovery and emergency action plan are the American Red Cross online guide at <<http://www.redcross.org/services/disaster/beprepared>> and the Federal Emergency Management Agency emergency planning publication at <<http://www.fema.gov/library/bizindst.pdf>>.

### Extraordinary events

The events that we typically think of as "disasters" aren't the only ones that can disrupt your practice.

**Medical emergencies.** For example, you should be prepared for medical emergencies involving an employee or client. Train employees in CPR and put procedures in place for reporting emergencies so help can be dispatched as

quickly as possible.

**Bomb threats.** Bomb threats are disruptive whether genuine or not. Develop procedures to determine whether you should evacuate the office. Most law enforcement agencies can provide you with a list of questions to ask the caller to help determine the seriousness of the threat.

**Workplace violence.** A violent intruder in the form of an angry adversary, disappointed client, or disgruntled former employee is a possibility in any law office. Create procedures outlining what to do in case of an attack. For example, consider limiting public access to one door. If the receptionist is vulnerable, develop a way for her to alert others in the office.

**Communication failures.** Communication failures can cripple your operations. Know who to call in the event of a failure. With the 800 number maze these days at telephone companies, you may have a difficult time getting service unless you have the proper information at your fingertips. Know who to call for which failures, whether it's local service, long distance service, Internet providers, and equipment providers. Also, develop interim procedures to use when your phone lines are down. For example, call-forwarding your main line to a recorded message will notify callers you're experiencing difficulties.

**Vandalism.** For vandalism that occurs during a break-in, security systems and interior locked doors after hours are the best deterrents. But what about unintended vandalism resulting from employee error or family members of employees visiting the office? I know of

an incident where an attorney's young child went into the computer room and disconnected all the cords from the patch panel. It took them several days to get their phones and computers back. Simple procedures such as restricting access to certain areas, or – in this case – having a map of the wiring locations can save untold hours of recovery.

**Office scams.** Office scams can cause considerable frustration and cost you dearly. Watch out for the toner pirates, the public safety fundraisers, the phone scams, the advertising scams (particularly the phony Yellow Page listings) and the latest favorite, the final-notice notifications – usually by fax – that your Web address is about to expire. They are extremely official looking, but if you read carefully you'll find that they're marketing dot-info addresses, not dot-coms. The best defense is to put procedures in place allowing purchases to be made only by a designated person, at least when buying from telemarketers.

Unfortunately we can't prevent most disasters, but we can certainly prepare so that they have less impact on our businesses. ■

---

*Paul Sullivan is the office administrator of Quinn Johnston Henderson & Pretorius with offices in Peoria and Springfield. He is a charter member of the Central Illinois Association of Legal Administrators and the ALA Cyber chapter and serves on the ISBA Law Office Economics Section Council. You can send comments, questions, or other correspondence about the column or any office management issues to him at <[psullivan@qjhp.com](mailto:psullivan@qjhp.com)> or 227 NE Jefferson, Peoria, IL 61602.*