



## **Is Your Firm Prepared to Cope with a Disaster?**

Tom Tamburino, account manager, RainMaker Software, Inc.  
[www.rainmakerlegal.com](http://www.rainmakerlegal.com)

**"Of all businesses that close following a disaster, 25% never re-open."**

In today's digital age, it is imperative to have a Disaster Recovery or Business Continuity Plan in place in the event of a disaster. When discussing disaster planning, we often think of disasters in the context of a hurricane, tornado, flood or fire, but a disaster can also be a crashed hard drive without a back-up or a back-up that can't be read. Being prepared and vigilant is the key to recovering from any disaster.

### **Prevention**

It has been said, "A disaster plan's success is best measured by its lack of use." Prevention begins with good housekeeping:

- Keeping areas free of obstructions and eliminating potentially overloaded circuits is an easy first step. Often employees bring in space heaters, fans, coffee pots, radios and clocks, any of which could cause an overload and fire.
- Observe physical security procedures. If you have restricted access areas, don't allow "tailgating" where one employee follows another into an area without swiping their card-key.
- Collect keys from ex-employees and notify building security when an employee is terminated or resigns.
- Observe information security procedures. Are passwords taped to monitors? Are laptops secured at the end of the workday? Does your staff leave open access to their computers at the end of the day or when they go to lunch? If so, is there a password on their screen saver? Is critical data allowed to be stored on local disk drives and are those drives backed up?

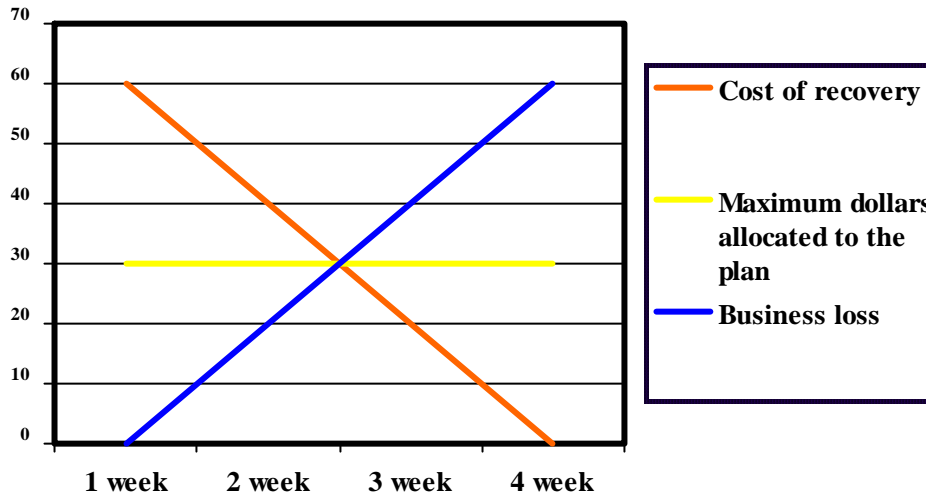
In the case of a hard drive crash, there is really no excuse not to have a back-up. More often we hear that the firm does a nightly back-up, however when the firm attempts to restore they find the tape cannot be read. There are a host of reasons why a bad back-up can occur, but firms can protect themselves by periodically doing a test restore from back-up tapes to insure they are readable.

### **Risk Assessment**

In order to conduct a risk assessment, you must analyze the possible consequences of a disaster. Examine your current state of readiness and look for weaknesses. Review insurance policies, emergency evacuation procedures, alternate work sites and information and document storage. Present your findings to the partnership and get their buy-in for a contingency plan. Two important factors to consider are; the amount of time they are willing to accept a disruption in their business and how much they are willing to spend to insure the disruption does not exceed their time frame. The combination of these two factors results in the 'Recovery Continuum', as depicted in the graph below. The time to recover is directly affected by the cost to

recover and the dollars allocated to the plan; recovery occurs where the lines intersect.

### Recovery Continuum



### The Business Resumption Plan

The first step is to assign a Plan Coordinator. Your first thought is probably to assign the position to your IT Director but, depending on the extent of the disaster and recovery effort, your IT Director may have his or her hands full trying to get your systems back on line and may not have time to coordinate individual departmental recovery efforts. The next step is to form teams and assign a team leader; this works best by creating teams within departments.

- Each team is responsible for gathering and maintaining their contact information. This information should include contact information for employees, vendors, key clients, other business partners & support providers as well as businesses who can provide disaster aid.
- Select a team meeting place, not too close to the workplace but also not too far, and have an alternate. Consider vulnerabilities, if your work place is in a low lying area prone to flooding, choose a location to meet that is on high ground. Make sure you have adequate communication capabilities and the size of the facility can accommodate the entire team. This meeting place is a place to assemble and coordinate recovery efforts; it is not intended to be a replacement work place.
- Create a critical records list. Consider, "If I cannot get into our office, what do I need to do my job?" Then create a list of critical items to retrieve if you are allowed to enter your building for a short period of time (which could be as little as 15 minutes). Because you may be under a time constraint when you enter your building, make sure the critical items are prioritized on the list.
- Select a method for protecting or reproducing information:
  - Electronic Records – Back-up & Store Off-Site
    - Don't store records too close to your facility. (For years many firms stored backup tapes in the vault of the bank on the first floor of their building. Many firms learned a terrible lesson on 9/11/01).

- Consider using a remote back up facility where your data is backed up over the Internet to a data storage facility that could be in another state. Most facilities provide 24/7 access, should you need to recover data.
- Paper Records are not as easily handled. Your choices are:
  - Duplicate and Store Off-site – expensive in hard dollars and staff time.
  - Fire Resistant Safes and Cabinets – offer some protections.
  - Re-acquire From the Source – although this option may seem outrageous, it may be the least expensive and most practical recovery method for most paper records.
- Create a Recovery Box and **store it off-site**. It should contain:
  - The Recovery Plan.
  - Staff, Vendor and Client Information.
    - Include all insurance policies (numbers & contacts).
      - General Liability, Health, Disability, Workers Comp, etc.
    - Contact information for companies who can provide aide in the event of fire or flood.
  - Critical Records List/Inventory.
  - Procedures Manuals.
  - Forms & Supplies Needed Immediately.
  - The list of critical items to retrieve, should you be allowed back into the building for a short time.

In the event of a disaster, remember that “Business as Usual” will be suspended

- Limited Operations
  - Can extend for up to a week or more
  - Set priorities and recover in phases
- Makeshift Operations
  - Can last for several months until normal operations are restored

In Summary:

- Top management establishes the guidelines.
- Identify serious risks.
- Prioritize operations and how to maintain them.
- Create disaster teams.
- Take a complete inventory.
- Know where to get help before you need it.
- Document the plan.
- Review often, revise as needed, train everyone, test periodically.

A “Disaster Planning Guide” including all forms and a plan template is available at no cost by contacting [ttamburino@rainmakerlegal.com](mailto:ttamburino@rainmakerlegal.com).

### **About the Author**

Tom Tamburino has been with RainMaker Software for 31 years and during his tenure he managed the disaster planning at the RainMaker data center that ran around-the-clock operations; supporting hundreds of law firms around the United States, Canada and Latin America. Since that time he has presented numerous sessions on the topic of disaster planning and business continuity. If you would like to learn more about how [RainMaker Software](http://RainMaker Software) can help your firm to improve operations, contact Tom directly at [ttamburino@rainmakerlegal.com](mailto:ttamburino@rainmakerlegal.com).