

# Open For Business: Disaster Recovery Plans Save Small Businesses

By Michael Doherty

I was sitting in my office contemplating the present state of the economy, while sorting through a variety of spam-emails promising financial wealth, greater virility and scantily clad women, when suddenly, my computer stopped responding. Despite anti-virus software, a worm had slipped through and was chewing up all the available memory on my hard drive. As divine intervention did not seem to be forthcoming, I called a tech savvy friend to beg for help.

*"It's okay, when's the last time you backed up?"* he calmly asked.

Now, I have an external drive connected to the computer and a plethora of re-writable CD's from my latest excursion to Costco, but as for actually backing up the system? Well, that would be last June, after the last time I trashed my files.

Does this sound all too familiar? For anyone who has spent days and weeks trying to recover from a computer disaster, imagine if a real disaster strikes. Are you prepared for the loss of customer and operational data? Can your business survive? Sure, advanced data recovery techniques can retrieve data from hard drives that have been in fires or under water for long periods of time, but data recovery services aren't cheap. Typical fees to recover data from damaged hard drives can range from \$300 to \$2,600 per drive exclusive of shipping. Research from the Gartner Group suggests that two out of five companies that experience a catastrophe or an extended system outage never resume operations. Of those that do recover, a third are out of business within two years. While the September 11 World Trade Center tragedy resulted in a horrific loss of human life and potential, it caused very little data loss due to the nightly backup practices of many Wall Street legal and financial firms.

Business continuity in its purest form hides inner chaos from the outside world. This business truism is perfectly encapsulated in two pithy sayings credited to Lucy Madeira, founder of the famous Madeira School. Lucy said: "function in disaster, finish in style," and "keep calm at the very center of your being." This implies that reputation will be preserved, business revenues undiminished, growth continuous and competitive edge maintained. The time and resources you've invested in building your business and all you've worked for will not literally go up in smoke. However, you must *plan* to recover from disaster.

It's important to remember that business interruption caused by a disaster can happen to any business, at any time. But you don't have to be statistic. With a few simple steps, you can avoid it. Careful attention to contingency planning in advance of a disaster is the key to rapid recovery and customer retention during or following a disaster:

- How would you operate your business tomorrow if a computer or facilities disaster happened tonight?
- How would you assess the immediate situation?
- What systems and protocols are in place to communicate with employees and customers?
- How well have you backed up crucial enterprise data, payroll, employee and tax information?
- Will the systems that run your business run remotely?
- What will be your business location for employees and for customers if your current facilities become unusable or inaccessible?
- Does your emergency preparedness plan address suppliers and other close business relationships?

The clarity and confidence with which you can answer these questions could be the difference between a successful recovery and a business failure.

## **Assessment**

The first step in an adequate contingency plan is an accurate assessment of your company's day-to-day business activities. After taking a hard fall, you want to have an accurate count of your fingers and toes. Companies must determine which resources (data, personnel and physical) are most critical to vital business activities.

- What would you need from a replacement facility in order to continue operations?
- How will you contact employees?
- Which job functions could be accomplished by temporarily telecommuting?
- Are your systems secure, redundant, and remotely deployable?

## **Communication**

Your employees are crucial to your business survival and clear communication will ensure their safety and effective action in an emergency situation. Much like fire drills, Disaster Recovery plans give each member of your organization comfort that he or she will be able to act in the best interest of themselves and the organization if the unthinkable happens.

- Meet with your employees twice a year to review emergency plans.
- Make sure you have a contact name and number in case an employee is injured.
- Make sure your employees know what to do if there is a telephone outage (have a back-up number elsewhere).
- Develop a notification protocol among the employees in case of emergency. Prepare a call list of essential employees. Include telephone numbers and home addresses.
- When the phones go down, you may have to send someone to transport the employees to your business location.

## **Customers**

Your customers represent cohesive relationships built over years. They will be sympathetic and patient with you, but you must be forthright with them. The more you do to ease the impact of your situation on customers, the more likely they will be to stick by you.

- If you can't provide goods and services to your customers, work with them to provide alternative resources until you are up and running again.
- Contact local media outlets, such as newspapers and local television stations, so you can assure your customers that you have reopened or that your business will be reopening soon.

## **Data Backup**

Studies indicate that 70 percent of American businesses probably backed up their computer records, however few might take the next step -- making sure the backups work. Test the system to see if it can read the stored data.

- Do you know where all of your company's crucial data files are located?
- How are these files being backed up?
- How often are these data backups run, verified, and tested?
- What kind of automation and controls are in place to make sure that data backup jobs run correctly and consistently?
- How often do your data backup tapes go off-site?

- Make sure your on-site computers have surge protectors or an uninterrupted power supply device, so that your data will be protected in the event of a power outage.

## **Records**

The more information you can access after a disaster, the faster you'll recover. You don't want to rebuild your database, while you're rebuilding your company.

- Make back-ups of all your company records and maintain them offsite.
- Some experts recommend that off-site storage be at least 50 miles away from your facility.
- Regularly back up payroll, tax, accounting, production records and customer lists.
- Keep your inventory list current and consider making a photographic or videotaped record of your inventory.
- Keep some hard copy records, such as your lease, insurance policies, etc. in a secure location (and photocopies of these in a different location).
- Identify information that may be recovered elsewhere, such as property deeds, bank information, or tax information housed with a contracted accounting firm.

## **Systems**

Consultants such as Gartner and IDC recommended that companies ensure they can manage their systems remotely. Insuring remote access for critical personnel involves several things:

- Make sure that you have the means to access your systems. This includes making sure you have computers that have the capability not only to tie in to the enterprise system, but also have enough processing power, storage and the applications needed to do their jobs.
- Insure people have the appropriate passwords and permissions to do what they need to do remotely. This can involve a balancing act with security considerations, especially in the case of administrators, because it means a direct pipeline into your systems from outside the enterprise offices. You may want to explore having a special mechanism to grant remote administrative privileges that can be activated in the event of an emergency.
- Plan and test to make sure you can use the remote access features when you need them. As part of your disaster-recovery planning, you should decide who needs remote access, on what level. Then test to make sure those people have that access and keep the list and the permissions updated as needed.

Consider Outsourcing -- turning data and application hosting, management, security, backup, and recovery over to a managed service provider (MSP) that provides a level of security, expertise, and redundancy typically missing in most organizations. Know what options you can count on before you have to count on them. The old business adage is business is location, location, location. In this age of emails, wireless networks and telecommuting, your systems provide the key to the virtual flexibility and survival of your company.

## **Facilities –**

As important as connectivity is for your data, records and systems, be sure not to neglect planning for your physical location. Should your office become inaccessible or unusable due to a disaster situation employees will need computers phones and electricity if you are to continue through the immediate crisis.

- Designate an alternate meeting location for your employees in case your business location becomes inaccessible.
- Be sure that your alternative site is not served by the same electrical power grid or communications center as your primary facility.
- Ensure site diversification exists -- keep backup resources or running standby systems at sites geographically separated from primary activities.

## Suppliers

It pays to discuss emergency plans with your current suppliers, so they will know what to do if an emergency or unforeseen event affects their operations and visa versa. You are not the only one who could face disaster. Always have a back up for the essential elements that support your business.

- Consider making a small volume of regular purchases with a supplier outside your local area or a qualified one with which you do not usually do business. Making a habit of testing and expanding your supplier market will not only increase and diversify your relationships, but it may also lower your costs.
- Always have two or three alternative suppliers and resources.

## Insurance

The better you document your claim, the greater the chance a timely insurance settlement.

- Are your insurance policies current? Is the coverage adequate? Who do you contact to make a claim?
- Do you need flood insurance?
- Do you need earthquake insurance?
- Do you need Business Income and Extra Expense Insurance?

After a disaster, you don't want to start asking these questions.

In conclusion, the more you plan for events of disaster, the higher your chance of survival. This should be an ongoing part of business planning. Don't allow the Disaster Recovery Plan to become a stale document. Update the information in the plan (1) when facilities are changed; (2) when equipment is changed; (3) when staff turnover or growth occurs; and (4) at least annually. While the ideas in this article are by no means an exhaustive list, the areas discussed should provide a good basis as you start your business planning for the unexpected.

---

About the author: Mike Doherty, the founder of Doherty & Associates, has an extensive background in corporate investments, including the evaluation and underwriting of over \$100 million in venture debt financing for emerging growth companies. Prior to Doherty & Associates, he was a director at Third Coast Capital where he focused on originating and underwriting venture staged debt products.

Prior to Third Coast Capital, he was a principal of Southport Systems, Inc., a consulting firm advising clients on asset management, leasing operations and credit underwriting. In addition, he has served as portfolio manager for numerous leasing portfolios.

Mike earned a BS in Commerce from DePaul University in Chicago.

### **Doherty/Associates/Ltd**

A premier business advisory firm specializing in

***Building Companies Together.***

Headquartered in San Francisco

[www.dohertyassoc.com](http://www.dohertyassoc.com)