



*The following article appeared in the March 14, 2008 issue of New Hampshire Business Review.*

## **Is your business prepared for disaster?**

*The computer equipment and information critical to your business is most vulnerable to disasters*

By Marc Berthiaume

As a small-business owner it is easy to devote the majority of your time to running your business and not worrying about preparing for a disaster until it's too late. Business disasters come in all shapes and sizes. They can vary from data loss or a power outage to an e-mail virus, equipment failure or a weather related incident.

The computer equipment and information that is critical to your business is most vulnerable to disasters. Businesses today rely heavily on computerized information systems. According to Jon Toigo, a 25-year veteran of disaster recovery planning and a well-known industry analyst, "companies denied access to mission-critical data for longer than 48 hours tend not to exist after one year. Those who plan have a four-times greater chance of survival than those who don't."

The U.S. Department of Labor estimates over 40 percent of businesses never reopen following a disaster. Of the remaining companies, at least 25 percent will close within two years. It is imperative that business owners ask themselves, "Is my company prepared for disaster?"

Typically, business technology solutions are immediate and reactive. Whether your business has five or 250 computers, it is important to switch your approach to information technology from a reactive fire-fighting approach to a proactive, preventive approach that identifies and addresses issues before they negatively impact your business.

Developing a disaster recovery and business continuity plan is an important proactive step all business owners should take. A typical disaster recovery plan addresses issues such as:

- Developing a formal (but workable) process to follow when a disaster occurs
- Implementing back-up and off-site data storage strategies to decrease risk of disaster
- Outlining strategies to begin recovery following a disaster
- Maintaining proper insurance coverage

### **Where to begin**

Information-gathering and assessment of risks are the first steps in creating a disaster recovery plan. To begin, a business owner must gather in one location information about the company including an organizational chart showing names and positions, a list of staff, suppliers, professional advisers and emergency services with contact information, maps of the premises and floor plans, asset and IT inventories, copies of all software and their respective licenses and insurance information.

Next, it is important to take time to assess the potential risks to your company so that you are well prepared in advance of a disaster. Any event that disrupts your business can potentially lead to disaster. Threats may include environmental disasters (floods, snowstorms, fire, etc.), equipment failure, security incidents and deliberate disruption.



Based on the information you have gathered, strategies and solutions that address each of the identified risks and threats to your business need to be developed. These strategies must be user-friendly and readily available to the key employees who will implement them when disaster strikes. Each and every disaster is unique.

Following a disaster, it is critical to take time to review the lessons learned and incorporate them into the next version of the plan. Among the threats to your business's computer systems are:

- Power outage
- Data loss
- Network exposure
- Water leaks
- Floods
- Fires
- Snowstorm
- Freezing conditions
- Web site availability
- Internal and external sabotage
- Ice storms
- Theft
- Hackers
- Equipment failure
- Labor disputes
- Communications services breakdown