

COMPUTER DISASTERS...ARE YOU CRISIS-READY?

by David Edwards, Bennett/Porter VP of Operations

"My data just disappeared...."

"My hard disk crashed and I haven't backed up in several months."

"We got a virus and lost our data"

"We relied totally on our IT Manager. He quit, and now we haven't a clue what's going on".

Computer site failures are common-place, and yet despite several recent natural disasters such as Hurricane Irene, which caused massive floods, power outages and untold billions in damages, more than half of small businesses (57 percent in a new survey) said they did not have a disaster preparedness plan for their business data.

According to a poll conducted by Carbonite, a provider of online backup systems, small business owners ranked the permanent loss of data as the No. 1 challenge to maintaining their business in the event of a natural disaster. Yet more than half responded that they had not created a disaster plan because they "haven't thought about it" - even though they believed that they would lose money if their business could not function for one day.

"Based on our recent study, small businesses recognize the value of protecting their business data and assets—but most are not adequately prepared for a data disaster," said Peter Lamson, senior vice president and general manager of small business for Carbonite.

In order to prepare for a computer disaster it is important to have a plan in place. Simple measures can be adopted to either avoid a disaster in the first place, or have a solid plan to help you recover in the shortest possible time. Two terms are used extensively when preparing a disaster recovery plan:

- The recovery point objective (RPO) is a defined point in time, prior to any potential disaster that might occur, from which *data must be recovered*. This point is determined by your organization after weighing the amount of acceptable data loss against the cost of additional Disaster Recovery Prevention
- The recovery time objective (RTO) is the maximum amount of time business processes can be down before they *must be restored* following a disaster (or disruption). This downtime includes the time spent trying to fix the problem without a recovery, the recovery itself, tests, and communication to the users.

The following table indicates three types of failure, varying from corrupt data to a complete site failure, together with typical times to recover:

Point of Failure	Summary	Recovery Time Objective (RTO)
Corruption of Data or loss of data	Probably the most common point of failure or disaster that almost everyone experiences	< 1 hour (If you have a tape backup it could be much longer)
Hardware Failure (Server/Workstation/Firewall, etc.)	Not as common but does happen on a periodic basis and should be planned for	4-24 hours if suitable replacement hardware is available 1 day or greater if suitable replacement hardware is NOT available
Complete Site Failure (Fire, Flood, or Other Natural Disaster)	Rare and not expected. Worst case scenario	1-4 weeks but greatly depends on availability of temporary location, and replacement hardware

So the moral of this story is to take adequate preventative measures to ensure you can recover your data should any of the above occur. For more information or for assistance with data protection and recovery, contact David Edwards at 503-225-9633.

David Edwards, as Vice President of Operations for Bennett/Porter & Associates, Inc., is responsible for managing a growing number of clients who rely upon the managed IT services that the company offers. This includes monitoring computers, ensuring all anti-virus software is up to date and helping clients prepare for disaster by providing off-site back-ups and professional IT staff to assist in recovering lost data.