By Rhonda M. Jenkins

Hackers, disgruntled employees, natural disasters, and even human error can wipe out millions of bytes of computer data - thousands of hours of work. Would your firm be able to re-create work product if your computer systems were unavailable for a few hours? What about days, weeks, months? If you're lucky, you may be able to reload your data from backup tapes. But you can't restore lost billable hours, or regain your client's trust and confidence if your critical computer systems are down for an extended period of time.

This article provides some general guidance for understanding, preparing, and hopefully avoiding, some of the common threats, and how to take the next step of developing a business continuity plan to help your firm survive should disaster strike. Having a disaster recovery and business continuity plan is analogous to having insurance coverage. You hope that you'll never need to use it, but you sure are happy that you have it when something bad happens.

What's at risk?
Whether its a common daily threat, such as a computer virus or a lost laptop, or a catastrophic event, such as fire, earthquake, tornado, hurricane, blackout, or terrorist attack, your business is at risk if your critical computer data is damaged or destroyed.

Today's law practice relies on its computer systems being available 24x7 to send e-mail, create documents, track billable time, maintain client records - basically everything we need to get our work done these days relies on having functioning computer systems. There's no turning back the clock - there's just no way to operate in today's business world without our computers.

Bad things do happen to nice computers
Described as one of the most disruptive computer viruses to date, the Blaster computer worm hit its peak on August 14, 2003. This nasty little critter raced its way across the Internet and caused hundreds of thousands of hours of computer downtime, and millions of dollars in losses to companies that did not have up-to-date virus protection software.

And, if dealing with a vicious computer worm weren't enough of a disaster, on the very same day, the entire Northeast section of the U.S. experienced one of the largest power outages in American history. Nearly 60 million people, and tens of thousands of businesses were left completely in the dark. The Northeast Blackout of August 2003 lasted many hours, and taught many a network manager the value of a good uninterruptible power supply (UPS).

An ounce of prevention
After the big Northeast Blackout of 2003, and once the Blaster worm died down, the businesses that were wise enough to proactively plan for these types of disasters were able to get their computer systems up and running, with barely a hiccup. Some of those who did not plan got a large dose of fried motherboards and corrupted data once the electricity started flowing. After the 9/11 catastrophe, everything changed - including the importance of disaster recovery and business resumption planning.

Developing an overall disaster recovery and business continuity plan can be a daunting proposition. Who has time to plan for something that might never happen? But, before you get overwhelmed and do nothing at all, you must weigh the risks in the context of your business. What would it cost your firm if something that might not happen actually does happen? And how long can you really plan to stay in business without your computers and data?

A disaster recovery plan can address some of these "what-ifs." Getting a plan in place doesn't have to be an all or nothing proposition that winds up getting stuck somewhere on the "I'll get to it when I'm not busy" back-burner. Your plan can be developed over time, starting with a disaster tolerant infrastructure. HP StorageWorks solutions offer a variety reliable network infrastructure products,
including fault tolerant network servers, tape backup systems, network attached storage arrays, and storage area networks (SANs).

And, should the disaster reach beyond the infrastructure, and your office is (gasp) unavailable for any reason, HP’s Business Recovery Services for the Office provides office work space, including desks, computers, laptops, telephone systems, expert assistance, proactive planning, and recovery solutions that can help you quickly get back to business with minimal disruption.

Protect thyself
HP offers a range of solutions to protect your valuable information and make your operations resilient. HP’s StorageWorks solutions include reliable tape backup systems, data protection, and disaster tolerant data storage solutions that can help keep your valuable information safe and sound.

At some point your computer systems are going to experience either a small annoying disaster (i.e. virus), or perhaps a major disaster. The "cross my fingers and hope it never happens to me" strategy is not going to fly. Protect yourself and your clients by getting your disaster recovery and preparedness plan off the ground with some of the basics:

- **Uninterruptible power supply (UPS):** A good UPS will provide an orderly shutdown of your network equipment in the event of a power failure, as well as condition the power. Look for a UPS that can support the total amperage of all of your network equipment, and that has a reasonable amount of battery life (15 min. or more). A good UPS will have software that will shut down your systems for you, and could cost anywhere from a couple of hundred dollars to a few thousand dollars, depending on size. A UPS is the single best investment you can make to reduce the risk of computer damage in the event of a power failure. HP offers reliable UPS's, surge protectors, and other power protection equipment for businesses of all sizes.

- **Surge protectors/line conditioners:** Not to be confused with a UPS, which provides emergency battery power, surge protectors handle spikes in electricity, which could fry a motherboard or other sensitive circuitry. Surge protectors are recommended for PCs, printers, modems, TVs, and other stand-alone electronic equipment. Line conditioners, which protect against fluctuations in the electrical current are a bit pricier, and generally not necessary for most PCs. But, line conditioners should be seriously considered in locations that commonly experience lightening storms, dirty power, or other electrical anomalies.

- **Dedicated circuits:** Even if you have a UPS, make sure that you plug it into a dedicated, grounded electrical circuit. This will ensure that your expensive network equipment is not sharing power with an energy- hogging appliance such as a refrigerator or air conditioning unit. Talk to your building engineer about the type of circuits that are running to your network servers and equipment.

- **Daily backups:** Tape backup systems copy critical data to a portable tape medium that can be restored on a different computer, or at another location. A daily backup routine is an absolute necessity in any disaster recovery plan. HP is the #1 tape storage manufacturer in the industry, and offers a range of reliable tape backup systems and software.

- **Verify backup restoration:** System backups aren't worth the tape they are written on if you can't restore your data. Perform periodic "data drills" where you restore your backup tapes to an alternate computer or at an offsite location.

- **Offsite storage:** Make sure you don't leave your backup tapes in the office; they could easily be destroyed right along with your computer systems. Even if you have a fireproof safe, tapes can melt if there's a fire. Send a set of backup tapes to an offsite location at least once a week, or just have the managing partner or IT person take the tapes home with them every Friday.

- **Select a disaster location:** Branch or satellite offices are ideal alternate locations to set up shop and resume business operations. Make sure that your offices have matching equipment,
like tape drives and file servers, so that you can quickly restore all critical software and data. If you do not have a branch office, use someone in the firm's home office. For larger offices, **HP's Business Recovery Services for the Office** provides expert assistance, proactive planning, and recovery solutions, including work space, desks, computers, laptops, and telephone systems.

- **Copy your CDs:** Your original software CDs and licensing information could be destroyed, and you might need to re-install your programs on another PC. Keep an offsite copy of every software title that you own, along with a list of all of the software license codes and registration keys. DVD writers, CD-R and CD-RW burners hold a lot of information, and are inexpensive way to duplicate your software, and even make backup copies of critical data that might be on local PC hard drives. **HP's DVD +R/+RW** devices hold up to 4GB of data, and are compatible with most popular DVD formats.

- **Update your software:** Nimda, Blaster, MyDoom, and who knows what's coming next. The scourge of Internet viruses and worms is an ever-present danger, which requires daily vigilance. Choose virus protection software that provides automatic updates. Also, make sure that you keep your operating system up to date with the most current security patches.

- **Keep your clients informed:** Keep copies of employee and client contact information readily available so that you can keep everyone in the loop about what's going on.

- **Partner with a seasoned pro:** With a track record of helping over 5,000 businesses recover from disaster, **HP's Business Continuity Services** comprise a range of solutions to protect your firm, including reliable tape backup systems, disaster recovery consulting and planning, offsite data recovery centers, and replacement equipment.

**Mitigating the risk**

It is impractical to plan for every possible contingency, but you can reduce your risk of exposure to system failure if you have an action plan. Property damage and business continuity insurance can also help mitigate the risk of a catastrophe, but insurance coverage is just one part of an overall disaster recovery strategy.

Many people incorrectly assume that their company's insurance coverage will somehow magically recover their lost data. Wrong assumption. An insurance policy cannot recreate destroyed work product, rebuild your time and billing system, or reimburse you for lost client confidence. After the catastrophic events of 9/11, many insurers are now requiring policyholders to undergo a comprehensive risk assessment analysis. Business insurance premiums and coverage limits can be affected by whether there is a disaster recovery and business resumption plan in place.

**Taking the next step**

Chances are that you already have some of the basic disaster recovery components in place, like offsite backup tapes and uninterruptible power supplies. The next step is to tie these basic IT recovery components into your overall disaster recovery and business resumption plan. To gain a better understanding of what further steps are required for your firm, take **HP's business continuity readiness assessment**. This assessment provides a list of things to consider during your disaster planning process.

**Failing to plan vs. planning to fail**

We might moan and groan, but we all obediently follow the floor monitor's directions and file out of the office like school kids when there's an office safety drill, because we know that emergency preparedness could help save a life someday. Computer systems and data don't rank nearly as high as human life. But, in the event of an emergency, you can't afford not to have a strategy that will allow you to recover your data, reassure your clients, and resume normal business operations. When disaster strikes, your ability to quickly recover could be the key to your firm's survival.
Rhonda M. Jenkins, formerly President/CEO of Legal Web Technologies, LLC, is currently working as an Associate Director with Navigant Consulting, Inc. The information contained herein is in no way intended to provide legal advice, and is subject to all of the terms of use of this web site.