

SBM

The Source for Business Owners

ST. LOUIS
**Small
Business
Monthly**

VOL. 16, ISSUE I

FEBRUARY 2003

What If Disaster Strikes— Is Your Technology Safe

by Wendy Gauntt

You hear it all the time—back up your data, scan for viruses, update your software—a steady drumbeat from the technology jungle. How many of us actually do all these things? The distant threat of unseen problems can't compete with more pressing day-to-day activities. However, with tight deadlines and limited resources, the ability to recover, or better yet, prevent disaster can make or break your small business.

Just how bad can it get? Let's review potential problems.

My Hard Drive Crashed

There are few moving parts in a computer that can wear out, but the majority of them are in the heart of your computer, its hard drive. And while reliability is very good, failures do happen. The key to an avoidable disaster is data file backup.

To recover, install a new hard drive, or, if your computer is a few years old, buy a new one. Once the new equipment is in place, reinstall your software from the original manufacturers' disks; then restore your data files from the backups that you made last night. You did make backups, right?

I Got A Virus From An E-mail

People know it's a risk, but when they find a fun program on the Internet, they often forward it to their friends, unwittingly propagating a new virus. Whoops!

If you are extremely cautious, you resist the temptation to open it, knowing that a malicious virus can completely wipe out your hard drive.

However, let's be realistic—most of us open e-mails from friends. What can you do to prevent problems? First, keep your virus definitions up-to-date by downloading new definitions off the Internet at least once a week.

Second, run daily virus scans. In most cases, virus protection software can remove an infection before it does serious damage. Worst case? You have to recover your data from backups after it has contaminated your entire network.

The Office Is Damaged By Fire

An electrical problem caused a fire in your office building. The parts of your office that aren't scorched are flooded from the firemen's efforts. What a mess!

It will take some time to recover from this one, but you thought ahead—you have good insurance and offsite backups (copies of your data stored somewhere other than your office). Most likely, you'll have to buy new equipment and then restore data from your offsite backups. Since you take backup copies home at least once a week, you only lose a few days of business activity.

Hacked By A 14 Year Old

Hackers, especially young ones, are constantly testing the limits of what they can do. Most small businesses have a number of vulnerabilities. If you've got an "always-on" Internet connection, such as DSL or cable, or if your employees have dial-up access from home, you are at risk.

The first line of defense is your firewall. A hardware firewall is placed between your Internet connection and your network; and a software firewall is installed on each computer. Consider the hardware firewall the deadbolt on the front door; the software firewall is the monitored alarm system. In a dangerous neighborhood such as the Internet, you want both.

Another line of defense is updating your software. Hackers covet security holes in popular software such as Microsoft Windows and Office. They exploit these holes to access your system, or to create specialized viruses that

take advantage of these vulnerabilities.

Most software manufacturers patch these holes quickly and make updates available on the Internet. Start by getting Microsoft updates: select "Windows Update" and "Office Update" at www.microsoft.com.

Reinforce your defenses with password protection. Network passwords should be a combination of numbers and letters not found in the dictionary and not easily guessed (no birthdays or pet's names). Create memorable passwords by substituting numbers for letters—"1" for "L", "3" for "E", "4" for "A", etc. For example, instead of "PASSWORD," write it "P455W0RD."

You can also secure specific drives, directories, and files with password protection; and, many software packages allow you to limit access to specific users.

Now The 25-Year-Old Hackers

While a 14-year-old hacker just wants to cause some havoc, a 25-year-old thief is likely to have a specific purpose, like stealing credit cards or gaining access to confidential information, such as salaries or medical records.

Sophisticated hackers use "social engineering," exploiting people's trust to gain access to their systems. These impostors might phone your office pretending to work for your tech support company, your Internet service provider, or your computer manufacturer. After building trust and rapport, they eventually ask for passwords. Never give out passwords no matter how credible the caller.

For a fascinating insider look at social engineering, check out "The Art of Deception," written by infamous ex-hacker Kevin Mitnick.

The Dishonest Or Angry Employee

While we like to think we work with good, trustworthy people, how can you be sure? Or

what if an employee is angry and wants to get back at the boss?

A dissatisfied employee can very quickly cause serious damage by deleting data files, corrupting your financial records, or downloading viruses to your network. Backup files are essential, but you can further reduce your risk by limiting employee access.

Secure confidential data files by setting up password-protected directories. Take advantage of built-in software capabilities to designate specific users for your financial and HR systems. Change your firewall settings to limit Internet downloads. Remove security access

from any employees who leave your company. Now that you've taken these precautions, take a step back...do your employees still have the ability to do their jobs? Too much security can create employee frustration.

In Summary

A little advance preparation and ongoing maintenance can mean the difference between an unexpected difficulty and a complete disaster.

- Backup your data regularly and keep copies offsite.
- Install a firewall if you have an Internet

connection.

- Run frequent virus scans using up-to-date virus definitions.
- Keep your software up-to-date by downloading the latest security patches.
- Secure your systems with passwords and limited user access.

The computer world has opened a wealth of business opportunities and efficient processes. Yet, be careful, heed the drumbeats, it's still a jungle out there.

Wendy Gauntt (wendy@cioservicesllc.com) is president of CIO Services, LLC.