Improve small business network data protection with tips from Microsoft Small Business.

Kim Komando writes about workplace technology and security issues. She's the host of the nation's largest talk-radio show about computers and the Internet, and writes a syndicated column for more than 100 Gannett newspapers and for USA Today. Find Kim's show on the radio station nearest you, and send an e-mail to subscribe to her free weekly e-mail newsletter.

By Kim Komando

You have auto and homeowner's insurance. But what about your computer data? The precautions needed to protect against disaster are like an insurance policy. You may not necessary ever need it but when you do, you're sure glad that you have it.

1. Install uninterruptible power supplies

This is the easiest thing you can do to protect your hardware and data. I'm surprised by how many people assume a surge protector suffices. But surge protectors only offer limited protection against power spikes.

For a better and more thorough protection, you need an uninterruptible power supply (UPS). A UPS isn't intended to power you through a blackout. (For that you would need a generator.) Rather, a UPS will let you save your work and power down safely.

A UPS contains a battery that is charged from a wall outlet. Your computer, monitor and printer get power through the UPS. The UPS cleans the power, so it's optimized. This is important, because power fluctuations can corrupt data. Most people only think of surges or spikes. But other fluctuations, such as sags in voltage, can be just as damaging.

When purchasing a UPS, make sure the power rating is right for your equipment. If you buy one that is rated too low, you might run out of juice before you can power down. Most UPS devices are designed to provide 10 minutes of power. If your equipment requires more power than the UPS is designed to provide, this time will decrease.

When selecting a UPS, you need to look at the VA rating — or amps multiplied by voltage (120v). The amp rating should be listed on your computer. Add up the VA ratings of everything you will connect to the UPS, then purchase a UPS with a VA rating 20- to-25 % higher.

When purchasing a UPS, be sure to look for UL ratings. This will ensure it has been tested for safety by an independent party.

Note: There are different kinds of UPS devices. For servers, buy an online UPS. (Online means outgoing power is always drawn from the battery.) This device is the most expensive kind, and it is about twice the price of other types of UPS devices.

Once attached to an online UPS, your server will always pull power from the battery. If the power fails, the server doesn't need to switch from one source of power to another. The net result: There isn't even a momentary interruption in power. Also, the battery buffer probably will protect you from lightning strikes.

If the battery in an online UPS fails, your server will still receive power. The UPS will bypass the battery and function like a surge suppressor.

Expect to pay between $150 and $1,000 for an online UPS. The higher the VA rating, the more you'll pay. There are other features that are nice to have but will raise the price. These include automatic self-test, automatic voltage regulation, audible alarms, overload indicator and building wiring fault indicator.

You might also want to consider buying one with advanced-battery features. These features include intelligent-battery management, battery-replacement indicator, and hot-swappable and user-replaceable batteries.

A line interactive UPS is less expensive. But when the power fails, it switches your computer to a battery and you will have a momentary power failure, which can endanger data.

Note: A UPS can also power down an unattended computer, and it can filter out electrical "noise" from network lines. This noise can slow data transfer and corrupt data.

2. Create a plan for backing up your data

Equipment can be replaced, operating systems can be reinstalled. But data is difficult and costly to recover.

For this reason, make it a priority for you and your employees to back up your company's data, and e-mail, regularly. You may want to back up anything else that is not easily replaced, such as custom programs.

One solution is to have employees save vital information on servers, not on workstations. Storing the data in a centralized location simplifies the backup process. You only have to worry about one or two machines.

The next thing to consider is frequency and types of backups. Here are three types of backups.

1. A full backup is just that: All files are included.

2. A differential backup includes files that have changed since the last full backup.

3. An incremental backup includes files that have changed since the last backup of any type.

There are advantages and disadvantages to each type of backup. Repeated full backups require a lot of space. Differentials use less. And incrementals are the smallest of all. But incrementals are the least convenient in restorations. Full backups are the most convenient. So you have a tradeoff between convenience and cost. All will work. It's up to you.

3. Decide what method to use to back up your data

Backup tapes, available at office and electronic stores, are popular. They're reliable and relatively inexpensive. However, there are drawbacks.

Tapes can be used and reused, but repeated use can degrade data. You need at least three tapes so you can rotate usage weekly. Then, if the tape is bad, you'll only lose one week's work. They won't last forever. So factor in the cost of replacement tapes. And make sure the tapes are spacious enough to hold all of your data.

Hard drives are cheaper. It's relatively easy to install a second hard drive on your computer or server. However, a second permanent hard drive is as susceptible to disaster as the original.

Another option is an external hard drive. These can be detached and moved to another location. They are offered in a range of sizes. Look for a one-touch backup.

You can also purchase removable hard drive bays or drawers. These provide the benefits of external drives, but are less expensive. You install a hard drive in an enclosure, and this enclosure slides into the computer. It is ideal for backing up large amounts of data.

Microsoft Windows includes a backup utility that can schedule operations. But you may want a more robust third-party program. This is particularly true if you're backing up Exchange server data or a large database. Exchange server data and databases pose a special problem because you need real-time backup.

You also must decide where to store your backups. At a minimum, a full backup should be kept offsite.

Online backup services are also popular. They will eliminate some logistical concerns. But online backups can be quite costly — especially if you have a lot of data.

With online backups, a control panel is installed on a computer. The administrator uses it to set backup options. Then, software is placed on all workstations and servers containing data. This software is used to back up the data on each workstation or server.

The data is compressed, encrypted and sent to a primary storage center. Often, another copy is sent to a second location for additional security. Prices vary, and many service providers offer free trials.

4. Maintain your backups

The most difficult part of the process is maintaining your backups. Certain steps can ensure that the process runs smoothly.

First, your backup utility should verify your data's integrity after backup. You might be tempted to skip this step because it's time consuming. (It can take as long to perform as the backup itself.) However, it will find any problems with the backup.

Secondly, you need to restore and test your data periodically. Again, this is time-consuming but worthwhile. To do this, rename the backed up folders on the original machines. Then, restore the backup and test the files by opening them. Important data should be tested regularly.

If you use tapes, clean the tape heads periodically. Also, check the backup logs for potential problems.

Make regular backups a habit. You'll sleep easier knowing your data is safe.