

## **Data Protection: Backup Strategies and Equipment**

In business, data is money. In the retail business, data can literally be money in the form of transaction data and customer accounts. It is equally valuable in the form of pricing, inventory data, and personnel records.

If data is money, then your computer hard drive is, in essence, the safe. The job of the hard drive is to store this information and present it to you at your convenience. Unlike a safe, a hard drive is not forever; they fail. If the data is not protected, it is lost.

### **By the Numbers**

- One hard drive out of 100 will fail in its first year.
- About 50% of all hard drives will fail within their first five years of service.
- About 50% of small business users have an effective backup strategy.
- The other 50% will have substantial unexpected data loss.

### **Strategies**

There are many degrees of data protection, all involving the duplication of the data on some other media or device. Strategies fall into two general categories, On-line and Off-line:

**On-line** – Some backup methods are in place continuously, duplicating the data on the fly to another device. The most common form of on-line backup is called drive mirroring, where two drives are constantly synchronized. Any change in one drive is instantly duplicated in the other drive. When one drive fails, the other takes over until the failed drive is replaced and the drives synchronize again. There are variations on this concept spreading the data across three or more drives for even higher reliability.

On-line strategies offer the advantage of a relatively automatic backup. There is no care or attention required until a drive fails. The cost of hard drives has fallen greatly in recent years making this one of the most economical strategies.

On-line backup, however, does not protect against a catastrophic failure (fire, flood, theft, power surge, etc...) nor does it offer any recourse from a computer virus problem. If a virus infects the system, the on-line system dutifully copies the virus to the backup drives as with any other data. Along the same line, an accidentally erased file is erased immediately on all drives.

## ***Strategies (continued)***

---

**Off-line** – An off-line strategy copies data to a data cartridge, CD or external hard-drive. Typically, data is copied at the end of the business day providing a ‘snapshot’ of the data at that time. A rotation strategy can be used with a number of data cartridges (CDs, external hard-drives) allowing the system to be ‘rolled back’ to a point before critical files were lost or damaged, even if the damage was not noticed immediately.

The major advantage of off-line backup is the ability to go back in time before the crisis occurred. Of course, the backup media is removable so the data can be stored off-site, safe from theft, fire, flood or other disasters. An off-line backup strategy, however, requires daily attention to swap cartridges or devices.

## ***Equipment***

---

**On-line** – The equipment for an on-line backup strategy is fairly basic; an extra hard drive and a controller card. The equipment can be purchased as part of the computer, or installed later. In a simple two drive strategy the computer needs to be shut down briefly to change the failed drive.

Server computers often utilize a special type of protection called ‘RAID’ (Redundant **A**rray of **I**ndependent or **I**nexpensive **D**isks). RAID based systems can run continuously even if a drive fails. Drives can be replaced easily without shutting down the system.

**Off-line** - Until recently, tape cartridge was the only off-line backup option. The tape drives are expensive, as are the tape cartridges (approx. \$50), which require frequent replacement. Tape backup can be less reliable than newer methods. However, tape backup is the only option for older computers running the NT operating system.

Backup to CDs and DVDs can be an excellent low cost alternative but they do not have the storage capacity of other methods. There is a new DVD technology which, when standardized, will hold about 20 gigabytes per disk, a similar capacity to a tape cartridge. At present, however, CD/DVD backup is only practical for smaller operations.

Another recent development has been the USB portable hard drive. Essentially, this is a standard hard drive in an external case that connects to a computer's USB port. With this method, the drive can be connected, disconnected or swapped at will, without disturbing the computer operation. The data 'snapshot' is copied quickly and easily onto the hard drive and then the drive can be disconnected and secured on or off-site as desired. The user can use multiple hard drives to establish a rotation. The falling price of hard drives and convenience of the USB connection are rapidly making this the most popular method for small and medium sized operations.

A variation on this concept connects the portable hard drive directly to the network allowing multiple computers to backup to the same device.

One final off-line method simply copies the data from the server to another computer on the network. This method costs virtually nothing, but the data cannot be taken off-site because it has simply been copied to another computer. Thus, this method offers little protection against theft or physical disaster, fire or flood.

## ***Making a Choice***

---

On-line offers excellent protection against a system crash but offers little in the way of archive or off-site protection. Off-line methods do nothing to prevent a system crash but are the key to recovering from a crash or catastrophic event. The best overall plan is to use a combination of both methods.

On-line drive mirroring is recommended for every system. The equipment is affordable and reasonably easy to install. Off-line storage for an older system means a tape drive. The USB hard drive seems to be the best solution for newer systems.

## ***Best Practices***

---

The best form of data protection is prevention. The leading causes of computer hardware failure are over-heating and poor quality power. Make sure your computer has plenty of ventilation. Squealing or squeaking noises are the signs of a failing cooling fan and should be investigated immediately. Computer equipment should be protected, at minimum, with a quality surge suppressor. Consider power filters and battery backup units for 'mission critical' computers.

- ∅ On-line mirrored and RAID systems are essentially transparent and require no attention. If a problem develops, a warning will appear on the screen and an alarm may sound. This typically indicates a serious problem and should be addressed immediately.
- ∅ Tape drives should be cleaned with compressed air weekly. An approved cleaning cartridge should be used monthly. Do not leave the tape 'stored' in the drive; it shortens the life of both the cartridge and the tape drive.
- ∅ Always choose the verify option for backup jobs. Although they will take longer, the verify pass will assure a quality job.
- ∅ Virtually all backup programs can be scheduled to run when the computer is otherwise idle. Be sure the backup does not conflict with other tasks such as virus scans and other scheduled tasks.

## ***Your Next Step***

---

Contact your NCBP representative for an analysis of your data protection needs.