Linotype-Hell

Technical Information

Protecting Your Data

Many users can’t afford (and in reality, don’t need) the non-stop or highly fault tolerant systems described in the article entitled *Fault Tolerance* (which appeared in the 1993 Linotype-Hell Technical Information notebook). For them, system administration that includes consistent backup, virus protection, and data recovery can protect against major data loss.

Backups

The most basic method of data protection is backing up. Backup[1], whether by tape, removable cartridge, rewritable optical, or floppy disk, protects data from loss due to component failure or deletion. All data must be backed up. Even fault tolerant systems require data backup because fault tolerance doesn’t protect from fire or flood, nor does it protect from data deletion. Similarly, the best RAID (Redundant Arrays of Inexpensive Disks) system cannot protect data from unintended deletion. Of course, since backup is not always a continuous process, there will usually be a window of time between backups where data could be lost. But the loss of a day or week’s data is certainly preferable to total loss. To make the backup disaster-proof, it should not be stored in the same location as the original file.

Two common types of backup are image backups and file-by-file backups:

- An **image backup** is an exact bit duplicate of the disk and when restored does not include any changes made since the backup was done. Image backup is sometimes preferred in troubleshooting when you are trying to get an exact duplicate of a customer's machine.
- A **file-by-file backup** allows you to restore an individual or multiple files should they be lost or damaged. This type of selective restoration is not possible with image backup.

Backups may be performed at the workstation level or at the file server level, depending on the type of server and backup hardware or software in use.

Computer viruses

A computer virus[2] is a computer program which was created to accomplish a specific, often malicious purpose. Though there are conceptual differences between computer viruses, logic bombs, Trojan horses, and worms, the end result is often the same, that is, the program deletes data from the hard drive.

- A **logic bomb** is a short program which is added to or modifies an existing program. It is set to explode when certain conditions are met. Logic bombs are often left by insiders, sometimes disgruntled employees who wish to wreak havoc on their employers. Logic bombs are less common in the Macintosh and IBM PC world than Trojan horses or viruses.
- A **Trojan horse** is a seemingly legitimate computer program that actually covers for a destructive partner. For example, a Trojan horse might contain a graphics program that displays nice images but which at the same time corrupts data on the hard drive. Trojan horses are activated when they are run on a computer system.
- A **computer virus**, while similar to logic bombs and Trojan horses, has the ability to spread to other parts of the computer or even to other computer

[1] The terms ‘archive’ and ‘backup’ are sometimes used as synonyms, but there is a slight difference. Generally, an archive provides a permanent record for future reference. A backup, on the other hand, provides protection if the original file is damaged or misplaced.

[2] A good resource on computer viruses is *Computer Viruses: What They Are, How They Work, and How to Avoid Them,* by Jonathan L. Mayo (1989, Windcrest Books, Division of Tab Books Inc., Blue Ridge Summit, PA 17294-0850). This book doesn’t cover some of the most recent developments, but it does provide a good overview, plus it takes historical look at some infamous computer viruses, including the Sunnyvale Slug, the Pakistani Brain virus, and the Cookie Virus.

systems. The term, however, may be used generically to describe all viruses, logic bombs, Trojan horses, and worms.

- A **worm** is a program which alters data in a computer's memory. A worm may only swap adjacent bits, but the cumulative effect can be devastating.

Protection from viruses

There are a number of ways to protect yourself from computer viruses:

- Be on the lookout for performance problems with your computer that may be a clue to a virus problem.
- Backup conscientiously.
- Work from write-protected disks.
- Don't let untrustworthy people use your computer. Even someone who copies a seemingly harmless game onto your computer may be opening the door for a computer virus.
- Monitor any software programs that you put on your computer. Don't accept pirated programs, beyond the utter illegality of it, a pirated copy may become infected while being passed from user to user.[3]
- Use common sense. A program that claims to be a word processor, and yet is very small in file size, say 10K, may be a virus in disguise.

Anti-viral software

The computer virus has become such a threat that all workstations should be equipped with the ability to detect, eradicate and protect from viruses. Regardless of the hardware and software platform, there is an anti-viral program that can provide protection at a minimal cost.

Some commercial anti-viral programs for the Macintosh include SAM (Symantec Anti-Virus), Disinfectant, and Virex. For the PC, two examples are PC Norton Anti-Virus and Central Point Anti-Virus. Some anti-viral programs are also available as freeware or shareware through electronic bulletin boards. To keep current with the latest viruses, it is important to keep up-to-date with the most recent releases of anti-viral programs.

Keep in mind that some anti-viral software may cause some problems with the automatic installation procedures of many software programs. (The actions of the installer may appear suspicious to the anti-viral program.) If you have problems installing a program, you may be able to resolve them by temporarily deactivating your anti-viral software.

Data recovery software

Many commercial programs allow you to recover files or entire disks that have been accidentally erased. These programs can be a godsend since no matter how much fault tolerance is built into a system, someone authorized to remove data can always make a mistake.

Data recovery has become so standard that several operating systems have the capability right into them. For example, MS DOS 5.0 has the ability to undelete an erased file and unformat a formatted disk. UNIX has fsck (File System Check) which checks a file system for integrity and automatically corrects any problems detected in the data structure of files and directories. Some common commercial data recovery programs include MacTools, PC Tools, and Norton Utilities for both the Macintosh and PC.

Acknowledgements

Many thanks to Eugene O'Brien for his help in producing this document.

[3] Be careful with any shareware or freeware programs you download from an electronic bulletin board system (BBS) or receive from a colleague. They may carry a computer virus. (Note: Most of the major on-line services check for viruses in uploaded files.)

Please direct any questions or comments to: Jim Hamilton, Marketing Department, Linotype-Hell Company, 425 Oser Avenue, Hauppauge, NY 11788
(For subscription information on the Linotype-Hell technical information series, please call 1-800-842-9721.)

May 1994, Part Number 7031