

September 6, 1999  
Government Computer News Vol. 18, No. 29

## Human Error Is the Culprit in Data Loss

By Drew Robb  
Special to GCN

Recent studies suggest that user errors and hardware failures do more damage to organizations' data than the hacker attacks that draw the headlines.

Not only are there more users every year, but users' computer literacy lags behind the growth curve of new hardware and software. Network flubs have the most devastating consequences.

Some experts have suggested that users themselves damage three times more data than do viruses, floods, lightning, earthquakes and hurricanes combined. The results of user errors include incorrect disk formatting, botched software installations, faulty or missing backups, improper shutdowns and, most common, accidental deletions.

A 1998 user survey conducted by 1-for-All Marketing of San Diego surveyed 115 subscribers to an online backup service and 195 general PC users. The federal respondents included Army Corps of Engineers users, federal prison officials and law enforcement officers, some of whom said they perform systems administration tasks.

Fifty-five percent of the respondents complained about users' accidental deletions and overwritten files. Only about three out of 10 said users learned the right lessons from their first mistakes.

More than half the 50 system managers in a separate survey by market researcher BNI of La Crescenta, Calif., reported dealing with accidental deletions at least once a month; some said such deletions occur daily. A missing file can take a manager anywhere from a couple of hours to several days to locate, so losses often go uncorrected.

### **Find It Or Else**

Even when a user has enough clout to order a search, the system manager might not be able to get the file back, depending on the state of current backups.

Some Novell NetWare, MS-DOS and early Microsoft Windows operating systems have an undelete feature. Microsoft Windows NT is a different story.

One surveyed PC user wrote, "I have just lost a week's work. I was using PKZip 2.04g in an MS-DOS Windows under NT 4.0 Service Pack 3. I was in a directory called d:\projects\cca\source. I typed the command 'pkzip-s1234567 source 980615.zip-m.'

"The system responded with a nothing-to-do message and, lo and behold, the entire directory was erased.

I searched the hard drive for any files that resembled the ones that had disappeared. No luck. ... Please, no comments about backing up. That is precisely what I was doing when it crashed.”

The user did not mention trying NT's Recycle Bin. It works well for local drives and picks up all files deleted from the Internet Explorer browser and from most Windows applications. But the Recycle Bin does not catch deletions from the NT File Manager, the command prompt, Shift-Delete or non-Windows applications.

Nor does the Recycle Bin capture deletions across a network. Malicious users could log into a workgroup's common files and delete to their hearts' content. Anyone with administrative privileges could erase much of an agency's operational information, accidentally or otherwise.

Backup tends to be the main method of retrieving losses on NT systems. But research indicates that up to 80 percent of users who regularly back up their data find the backups inadequate at critical moments. One study of 260 respondents found that 62 percent could not recover all the data they needed from tape backups.

Another survey by 1-for-All Marketing sought the reasons behind users' failure to recover all their data. Once again, human error overshadowed other types of failure.

There are several ways to combat backup shortfalls:

- Set up a backup verification procedure. Although it slows backup, verification ensures peace of mind. Test backup tapes monthly to see whether their data is fully available.
- Buy servo tape drive hardware, which improves data repeatability by inserting information in better positions. The servo information is either interspersed with data tracks or embedded at the start and end of a tape.
- Choose good-quality digital linear tape or digital audio tape media for backup. Linear-tracking DLT goes past the read-write head only once and is good for about 10,000 passes, or 100 to 300 backups. Each tape holds up to 70G. But the tapes and drives are expensive. A 4-mm DAT cartridge has a helical drive that increases the number of times the head crosses over the tape, making DAT more susceptible to wear.
- Some Windows NT backup programs can make complete or selective backups. There also are NT disaster recovery products, such as Replica Network Data Manager from Stac Inc. of San Diego and Seagate Storage Manager from Seagate Software of Heathrow, Fla. Two remote and online backup options are @Backup from @Backup Corp. of San Diego and Cheyenne ARCserve from Computer Associates International Inc.

Backup solutions, however, do not totally eliminate users' day-to-day recovery demands. Asking a network manager to search for one lost file on a backup tape is like asking NASA to launch the space shuttle to go around the block. And if a document was created after the last backup, it does not exist on tape at all.

A couple of utilities can do the same job as the old Undelete command in MS-DOS and Windows 3.1, and the NetWare Salvage command.

## **In The Has Bin**

The Norton Utilities suite for NT from Symantec Corp. of Cupertino, Calif., for example, has the Norton UnErase tool for use on local drives. Anything erased via the File Manager, Shift-Delete or a non-Windows application is caught and recoverable, though in a cumbersome way. UnErase sets up a recovery bin in addition to the Recycle Bin. When the user purges the Recycle Bin, all the files end up in the other bin.

The Norton recovery bin misses command prompt and File Allocation Table deletions, and it lacks network functionality—an important feature for system managers who would rather not have to hike to a specific server for a deleted file or install the utility on 50 servers. But it certainly beats dealing with multiple backup tapes.

Undelete from Executive Software International Inc. of Glendale, Calif., has a couple of features not found in

Norton UnErase. Instead of setting up an extra bin, it replaces the Recycle Bin entirely. It catches just about any kind of file deletion, including those from the command prompt.

An Energy Department office in Germantown, Md., has installed Undelete for 250 users of NT 4.0 and Windows 9x plus other operating systems such as NetWare 4.11, Red Hat Linux, SunSoft Solaris and Unix.

“Particularly during cleanup efforts, users often delete important files and sometimes even system-critical files,” one Energy system manager said. “I was restoring NT files from tape at least once a week.”

Because Undelete is networkable, the manager can now undelete erased files at remote locations without leaving his desk. An undelete-from-disk feature is part of the software installation, and Undelete on CD-ROM can serve as an emergency file recovery tool.

### **Monthly Tests**

“The essentials of loss prevention are good backup and restore procedures that are tested each month,” the Energy manager said. He also cited having RAID Level 5 storage and spare disk configurations for servers.

Despite the current scaremongering about viruses and year 2000 Armageddon, data loss from simple human error is too common to be swept quietly under the keyboard. Overemphasizing certain types of loss protection while overlooking user error leads to disaster sooner or later.

Drew Robb is a Tujunga, Calif., free-lance writer who specializes in business and technology.