This is the eleventh in a series of short articles reviewing the theory and practice of making backups.

***

Backup Archives, Maintenance and Retention

Having created a backup set, what should one do with it? The first thing to do is to test the readability of the data. Modern backup software automatically verifies the readability of backups; this functionality must not be turned off. When preparing for any operation that destroys or may destroy the original data, one should make two independent backups of critical data; it is unlikely that exactly the same error will occur in both copies of the backup. Such dangerous activities include partitioning disk drives, physical repair of systems, moving disk drives from one slot or system to another, and installation of new versions of the operating system.

Retention Policies

One of the obvious reasons to make backup copies is to recover from damage to files; however, there are also legal and business requirements for data storage and retention. For example, certain jurisdictions require seven years of business data to be available for audits by regulatory or taxation agencies. The corporate legal staff may advise retention of certain data for even longer periods as support for claims of patent rights or if litigation is envisaged. In all cases, the combination of business and legal requirements necessitates consultation outside the data processing department; decisions on data retention policies must involve more than technical resources.

The probability that a backup will be useful declines with time. The backup from yesterday is more likely to be needed than the same kind of backup from last week or last month. On the other hand, each backup contains copies of files which were changed in the period covered by that backup but which may have been deleted since the backup was made. Data center policies on retention vary because of perceived needs and experience as well as in response to the business and legal demands mentioned in the first paragraph of this section. The following gives a sample policy to illustrate some of the possibilities in creating retention policies:

* Keep daily backups for one month.
* Keep the end-of-week backups for three months.
* Keep the end-of-month backups for 5 years.
* Keep the end-of-year backups for 10 years.
Rotation

Re-using backup volumes makes economic and functional sense. In general, when planning a backup strategy, different types of backups may be kept for different lengths of time, as suggested in section 41.4.1. To ensure even wear on media, volumes should be labeled with the date on which they are returned to a storage area of available media and used in order of recovery (first in, first out). Whenever possible, newer media should be reserved for backup volumes destined for longer retention. An expiry date should be stamped on all tapes when they are acquired so that operations staff will know when to discard out-dated media.

In the next article in this series, we'll look at media degradation.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.