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

***

Data Vaults

Most enterprises will benefit from contracting with professional, full-time operations specializing in maintaining archives of backup media. Some of the key features to look for in evaluating such facilities include

* Storage facilities made of concrete and steel construction to reduce risk of fire.
* No storage of paper documents in the same building as magnetic or optical media storage.
* Full air-conditioning including humidity, temperature and dust controls throughout the storage vaults.
* Fire sensors and fire retardant technology, preferably without the use of water.
* Full time security monitoring including motion detectors, guards, and tightly controlled access.
* Uniformed, bonded personnel.
* Full time, 24 x 7 x 365 data pickup and delivery services.
* Efficient communications with procedures for authenticating requests for changes in the lists of client personnel authorized to access archives.
* Evidence of sound business planning and stability.

References from customers similar in size and complexity to the enquiring enterprise will help manager make a wise choice among alternative suppliers.

Online Backups

An alternative to making one’s own backup copies is to pay a third party to make automatic backups via high-speed telecommunications channels and to store the data on behalf of customers. Some of the firms involved in these services move data to magnetic or optical backup volumes, but others use RAID (ganged disks) for instant access to the latest backups.
Additional features to look for when evaluating online backup facilities:

* Compatibility of backup software with computing platform, operating system and application programs.

* Availability of different backup options (full, differential, incremental, delta).

* Handling of open files.

* Availability and costs of sufficient bandwidth to support desired data backup rates.

* Encryption for data during transmission and when stored at service facility.

* Strong access controls to limit access to stored data to authorized personnel.

* Physical security at the storage site and other criteria similar to those for data vaults.

In the next article in this series, we'll start looking at disposal of discarded backup media.

***

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.