Backups (17):  
Scavenging

by M. E. Kabay, PhD, CISSP  
Associate Professor, Computer Information Systems  
Norwich University, Northfield VT

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

** **

Before throwing out backup media containing unencrypted sensitive information, operations and security staff should ensure that the media are unreadable. This section looks at the problem of data scavenging and then recommends methods for preventing such unauthorized data recovery.

Scavenging

Computer crime specialists have described unauthorized access to information left on discarded media as scavenging, browsing, and Dumpster-diving (from the trademarked name of metal bins often used to collect garbage outside office buildings).

Scavenging is probably the third most important method of computer crime; the first two are data diddling and unauthorized use of computer services.

Scavenging can take place within an enterprise; for example, there have been documented cases of criminals who arrange for requests to read scratch tapes (tapes that are used for temporary storage of data) before they read them. These people were prospecting for tidbits of data left by previous users. Operations policies should not allow scratch tapes or other media to contain confidential data; all scratch media (including backup media that are being returned to the free list) should be erased before they are put on the media rack.

Before deciding to toss potentially valuable documents or backup media into the garbage can, managers should realize that in the United States, discarded garbage is not considered private property under the law, according to a U.S. Supreme Court ruling. Anything that is thrown out is fair game for warrantless searches or inspection by anyone who can gain access to the garbage without violating laws against physical trespass. Readers in other jurisdictions should obtain legal advice on the applicable statutes.

Under these circumstances, the only reasonable protection against data theft is to make the garbage unreadable.

In the next article in this series, we'll look at destroying backup data 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