Scavenging (1):
Garbage Out, Data In

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

Sometimes it's the little details that destroy the effectiveness of network security. Firewalls, intrusion-detection systems, token-based and biometric identification and authentication -- all of these modern protective systems can be circumvented by criminals who take advantage of what few people ever think about: garbage.

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).

Discarded garbage is not considered private property under the law in the United States. In 1988, the Supreme Court heard California vs Greenwood et al. in which a Mr. Greenwood argued that his arrest on drug trafficking charges was illegally obtained by warrantless search of green plastic garbage bags he had placed outside his home. However, Justices White, Rehnquist, Blackmun, Stevens, O'Connor and Scalia wrote,

"The Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home.... Since respondents voluntarily left their trash for collection in an area particularly suited for public inspection, their claimed expectation of privacy in the inculpatory items they discarded was not objectively reasonable. It is common knowledge that plastic garbage bags left along a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public. Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through it or permitted others, such as the police, to do so. The police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public....."

In other words, anything we throw out is fair game, at least in the US. Other readers would do well to determine the state of jurisprudence dealing with the privacy, if any, of garbage in their jurisdiction. The only protection is to make the data in the garbage quite unreadable.

Discarded information can reside on paper, magnetic disks and tapes, and even electronic media such as PC-card ramdisks. All of them have special methods for obliterating the unwanted information. I don't want to spend much time on paper, carbon papers, and printer ribbons; the obvious methods for disposing of these media are so simple they need little explanation. One should ensure that sensitive paper documents are shredded; the particular style of shredding depends on the degree of sensitivity and the volume of sensitive papers. Cross-cut shredders, locked recycling boxes and secure shredding services that reliably take care of such problems are well established in industry.
In the next few columns, I'll review practical recommendations for protecting corporate (and private) information in memory and on disks or tapes from snoopers. In the meantime, I suggest that readers take a look around their own operations and find out how discarded paper, electronic and magnetic media containing confidential information are currently handled. With this information in hand, you'll be able to read the upcoming articles with your own situation well in mind.

* * *


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. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 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.