Data Destruction

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University

One of the problems in calling a professor for a quick insight into something they teach is that it's hard to shut us up.

Recently a very nice reporter called me for comments about data destruction; later I wondered if she was appalled by the length of the interview.

I think that one of the essential steps in planning for data destruction is to have a complete and up-to-date inventory of the life-cycles of all the types of information held by an organization. The information we need is likely to be found in service-level agreements, backup policies, business-continuity and disaster recovery plans. We have to know how long each type of data should be kept, and for what reasons. Important factors in such decisions are legal and regulatory requirements. Over a decade ago, I wrote,

> Before engaging in any new data destruction, …[we]… would do well to consult corporate counsel to establish the legal requirements that contribute to determining appropriate data retention policies. Different classes of data will have different retention periods mandated by law, regulations, or business requirements such as due diligence investigations preceding mergers and acquisitions.< http://www.mekabay.com/nwss/133_data_destruction.pdf >

A primary concern among commercial organizations is that excessively long persistence of data increases the risk of expensive efforts to comply with court orders such as warrants and subpoenas. Having to search or even transfer orders of magnitude more data than necessary can be expensive in time and materials. In addition, old data fragments or repositories may no longer have the information to provide context for accurate interpretation of the old records. References which might explain apparently compromising memoranda may be missing, with dire results in court proceedings.

Another paragraph from that old article reads,

> Any change in policies on data destruction should be closely coordinated with the information technology group to be sure that backups and archives are included in the analysis. Electronic or optical archives of documents, including e-mail -- and including backups -- are a rich source of data mining during the legal discovery process. In addition, your client should examine the distribution of documents it wishes to destroy but which reside on employees' desktop, laptop or even personal home computers. Unfortunately, many users have no idea that copying company information onto their home computers poses a security risk; in addition, many novices store documents higgledy-piggledy in a single folder (e.g., "My Documents") with no subfolders, with filenames such as "Document.doc" and with empty property sheets that convey nothing about the subject matter or provenance of the documents. Finding and extirpating all copies of documents that ought to be destroyed may be much harder than it seems at first

glance.

Data destruction policies cannot succeed without data-loss prevention policies and appropriate controls to ensure that employees follow acceptable standards for extraction and storage of data from corporate sources. For one thing, copies of data downloaded from active data sources become out-dated; employees who, for example, extract customer data from a master database may find that their information is out of date within days or weeks – and that decisions or calculations based on the old data may lead to errors.

In today's bring-your-own-device (BYOD) environment, strict policies on data retention become increasingly important; we don't want a statement to the court about the destruction of specific data to be contradicted by forensic examination of employee-owned devices.

Another implication of data-destruction policies is that no data must be destroyed without justification – and in particular, no data must be destroyed when there is a court order in place or even expected in the immediate future. Data cannot be destroyed capriciously; selective deletion of specific email threads, for example, could be construed as evidence of attempting to conceal malfeasance.

As for the methods of data destruction on storage media, professional services (look up "data destruction" in a search engine) are an excellent choice for small to medium businesses. These firms can provide securely locked receptacles for paper, for discarded magnetic media, for optical media and even for hard disk drives. On a regular schedule, they can either pick up the discards for treatment at a central facility or destroy the media on the spot using large-scale shredders.

Speaking of shredders, if readers need to buy small- or medium-scale shredders for their homes or offices, they should be sure to buy *cross-cut* shredders that fragment media into little diamond-shaped pieces. Old-style parallel-blade shredders produce paper that can be pieced together too easily for comfort. One recent example of poor shredding was the discovery in late November 2012 at the Macy's Thanksgiving Parade in Manhattan that some of the confetti thrown around at the celebration contained confidential – and readable – information from files of the Nassau County Police Department.< http://newsfeed.time.com/2012/11/27/macys-thanksgiving-day-parade-confetti-made-using-confidential-police-documents/ >

* * *

A useful document from the US National Institute of Standards and Technology (NIST) that includes discussions of email retention policies is "NIST Special Publication 800-45, Version 2, "Guidelines on Electronic Mail Security" (February 2007). <

For more information about media sanitization standards , see Draft NIST Special Publication 800-88, Revision 1: "Guidelines for Media Sanitization" (September 2012).< http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf >

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *