With the popular and technical press reporting extensively on the Enron scandal, where data destruction is playing an important role in the interpretation of how Enron’s accountants behaved, it is not surprising that many organizations are reconsidering their own data retention and data destruction policies. A colleague submitted the following (edited) question received from a client:

“We are seeking your advice on the issue of how we destroy records. We’re currently working with various vendors on proposals and if shredding is determined to be a corporate policy, then a company-wide policy would be needed to achieve the best price. It would also determine the vendors we could deal with, since we might want a single vendor to support all regions. The paper-recycling companies won’t take responsibility for confidentiality of our data, since information security is not part of their business. In contrast, shredding companies will pick up discarded materials from locked cabinets and even transport materials in a locked truck if necessary; they accept responsibility for our information from beginning to end. Can we legitimately shift the liability and responsibility to a third party through the contract? Can you provide us with any industry standards on handling destruction and what companies are doing in light of the Enron issue or because of the growing emphasis on privacy? If the expectation is that shredding will become a preferred method for destroying customer information then we should push to clean things up in 2002 and budget for costs expected in 2003, when we would start shredding lots of materials.”

* * *

First, a mandatory disclaimer: I am not a lawyer and this is not legal advice. For legal advice, consult an attorney with expertise in this area of law.

Before engaging in any new data destruction, your client 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.

The idea of using a single contract for all sites is appealing: it ties into the principle that policies should be applied as uniformly as possible (with due allowance for special cases). For example, in a court of law, it would be tedious and even embarrassing to have to detail the precise data retention and data destruction policies for a dozen locations, each of which had significant but largely unwarranted variations in their practices.

As your client writes, specialized shredding companies do indeed accept responsibility for documents once they have control over the paper or other media; however, they cannot take responsibility for what is done to data before they are discarded. Since employees have by far the largest opportunity for data destruction, mis-filing, or theft, your organization will naturally
keep the largest responsibility for data confidentiality and face the greatest liability for compromise of confidential data – not to speak of losses incurred through data scavenging by industrial spies or criminal hackers. Remember that it will take time to train employees to use special lock boxes to discard confidential documents; many will, at first, continue unconsciously to throw sensitive documents in ordinary trash or to place them carefully in ordinary unprotected recycling bins.

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.

As for starting to shred documents on a large scale, there are some public-relations issues as well as legal issues to consider. Before engaging in any new data destruction, I would ensure that the IT and documents staff consult the corporate counsel to be sure that there are no legal proceedings anticipated. It would be embarrassing to have public disclosure of widespread data destruction, even though perfectly legal, just before a court-ordered discovery were due to start. That was precisely what happened in the Enron case before the court orders were served.

It will be critically important to ensure that nothing is destroyed that is in fact clearly useful or needed. In their enthusiasm for getting rid of superfluous materials, it is quite likely that some employees will go overboard and destroy documents that the organization actually wants to keep available. This risk is especially serious when people start the perhaps unfamiliar process of destroying magnetic or optical media. Many users have a lamentable habit of not labeling their diskettes, cartridges, tapes and CD-ROMs or worse, reusing materials with an old and incorrect label. If employees start throwing out these storage media without accurately evaluating the importance of the information carried on these devices, the organization may suffer irretrievable losses.

Organizations should lay out clearly understandable, unambiguous standards for electronic data destruction. It should be possible to go through a checklist that leads a user to a firm conviction that destroying a particular dataset is completely appropriate, completely inappropriate, or questionable. The questionable cases should be discussed with a supervisor. The unambiguous decisions should be documented so that the organization has a permanent record of what was destroyed in the cleanup. Now, excessive detail might defeat the purpose of the data destruction, so the data management guidelines should include examples of suitable notations for tracking the data destruction. The subject of dealing with criminal behavior is outside the scope of this response, but at the very least, management should make it clear in its policies that destroying data indicating criminal activity is _not_ a legitimate process and that the organization’s policies explicitly forbid cover-ups of any such criminality. In a well-run organization, any employee who has reason to suspect criminal behavior by colleagues and who is nervous about reporting such evidence within the chain of responsibility should be _encouraged_ to contact law-
enforcement organizations for help.

* * *

LINKS:

For a history of shredding, see <http://www.msnbc.com/news/696082.asp?cp1=1#BODY>.

The U.S. General Services Administration (GSA) has excellent guidelines on disposing of records at <http://gsa.gov/staff/c/ca/disp.htm>.


Another example of such standards is from the U.S. Department of Agriculture at <http://ardor.nara.gov/agricult/aphis/rmm-4.html>.

* * *

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.