



## Trash or Treasure?

**In light of recent court decisions and government regulations, it's important to understand the latest in effective document retention — *and destruction*.**

By Stephanie Doyle, Editor

Document retention used to be fairly simple. Employees shredded paper documents when they ran out of physical space, or dumped records deemed important into boxes for future warehouse storage. But new regulations and recent court decisions combined with a surge in electronic data have complicated the corporate record-keeping process.

"Organizations have to protect themselves to make sure they are striking a balance between destroying stale documents and adequately preserving important documents," says Michele Lange, an attorney with Kroll Ontrack Inc., which specializes in data recovery, computer forensics, and electronic discovery.

### COMPLIANCE

A risk exists each time a company retains documents that contain potentially harmful or sensitive information. An effective document retention policy helps ensure that everything a company must keep, is kept — as long as it is needed and no longer.

An effective policy allows a company to protect its assets — electronic files and confidential information, says Carlos A. Martínez Jiménez, corporate auditor for 3M México, the Mexico City operations of 3M Co. "It also gives us an advantage by having all of the documentation needed if we become aware of any legal issues involving the company." 3M Co., a diversified technology company, is headquartered in St. Paul, Minn., and has operations in more than 60 countries. An effective retention policy, says Martínez, ensures that each of those operations complies with local and global regulations.

Indeed, an effective document retention policy helps ensure compliance with state and federal laws, including the U.S. Sarbanes-Oxley Act of 2002. The landmark legislation imposed new requirements on public companies and their accounting and audit teams regarding the retention and destruction of certain records.

Peggy Fish, director of audit at Purdue University in Lafayette, Ind., says complying with Sarbanes-Oxley has advantages and disadvantages for those creating and implementing retention policies. "At least there are no gray areas in terms of knowing what you should and shouldn't be retaining when you're under regulation. On the other hand, it certainly does create some additional costs and burdens."

Either way, Sarbanes-Oxley has instilled in many companies a sense of document retention urgency. Section 802 of the act, known as the "Corporate and Criminal Fraud Accountability Act," states that anyone who alters, destroys, or conceals a document with the intent to impair the object's integrity or availability for use

### Top 10 Tips for Effective Electronic Data Management

1. Make electronic data management a business initiative, supported by corporate leadership.
2. Keep records of all types and locations of hardware and software in use.
3. When creating a policy, consider backup and archival procedures, privacy concerns, any online storage repositories, record custodians, and a destroyed documents "log book."
4. Create an employee technology use program, including procedures for written

in an official proceeding will face criminal penalties.

"Sarbanes-Oxley definitely has spurred a lot of folks into action, mostly because there can be a 20-year jail term associated with destroying documents — and that's scary," says Lange, author of *Electronic Evidence and Discovery: What Every Lawyer Should Know*.

## THE ELECTRONIC DOCUMENT

Sarbanes-Oxley and subsequent rules from the U.S. Securities and Exchange Commission require public companies, corporate counsel, and accounting and audit professionals to consider the impact of electronic evidence in relation to certain records. That's a challenge in today's digital age, where records can be created or destroyed with the click of a mouse, and relevant data can be scattered on personal computers and laptops, network servers, portable digital assistants, cell phones, and myriad electronic storage media, from hard drives to backup tapes.

"The digital data explosion is one of the reasons why document retention really has taken center stage," Lange says. "Today, nearly every electronic document we keep is being saved somewhere. We're not as aware of it because we don't see piles of papers sitting around. Instead, they're all saved digitally."

Unbridled use of technology has complicated record-keeping, Martínez says. "One of the most challenging aspects is the development of controls and processes to manage the amount of documents — hard copy and electronic. We have to consider information security as well as the records management services available in our company, which allow us to determine types of records, records inventories and record-retention schedules, particularly physical or electronic facilities that could provide low-cost storage for the company."

These days, a document can include just about anything. "It definitely includes e-mail and written documents, and it can include database records and, in some cases, cell phone text messages," Lange says. "There is little case law on instant messages, but I think we'll see more of that in years to come." The Judicial Conference of the United States, the policy-making body for the country's court system, has proposed amendments to the [Federal Rules of Civil Procedure](#). Among the proposed changes up for public comment is the definition of *document*, which could include an entire computer. "As technology changes and the way we communicate changes, corporations are going to need to keep abreast of that," Lange suggests. "More people are carrying Blackberry computers, and all of that information is going to need to be tracked."

Recent case law reveals that judges aren't hesitating to impose hefty fines against businesses and public institutions that don't handle or hand over records properly. A judge in 2004 sanctioned Phillip Morris USA Inc. US \$2.75 million for failing to keep and produce e-mails in a case that claimed the tobacco giant had marketed cigarettes to minors. "Two years had passed and hundreds of thousands of documents were destroyed," Lange says. Phillip Morris contended that employees simply continued to follow the document retention plan already in place. But when litigation begins or is reasonably anticipated, cautions Lange, the status quo must cease. That means placing a hold on document destruction routines. "When litigation commences, it's important to take adequate preservation steps."

## IMPLEMENTATION

Just how long should an organization hold on to each type of record? "That is the million-dollar question," says Lange. "It varies depending on industry. That's why it's so important to involve the legal team and records managers to make sure you are researching the applicable laws."

After first identifying required regulations, an effective document retention policy should clearly specify the retention periods for every type of document, says Gary P. Crispens, director of internal audit at the Virginia Department of the Treasury. "The most challenging aspects of records retention are the identification of the required holding period and the cataloging of the documents into a storage inventory."

communication protocols, data security, employee electronic data storage, and employee terminations and transfers.

5. Clearly document all company data retention policies.
6. Document all ways in which data can be transferred to and from the company.
7. Regularly train employees on the organization's data retention policies.
8. Implement a litigation response team — comprised of outside counsel, corporate counsel, human resources, business line managers, and information technology staff — that can alter any document destruction policy quickly.
9. Be aware of electronic "footprints"; "delete" does not always mean "delete," and metadata is a fertile source of information and evidence.
10. Cease document destruction policies at first notice or anticipation of a lawsuit.

— *Courtesy of Kroll Ontrack Inc.*

The Treasury Department's document retention policy is part of a statewide program run by the Archives and Records Division of the Library of Virginia. Hard documents, such as incoming and outgoing letters and faxes, annually are boxed up by type of document at the Treasury Department, and transferred to the Library of Virginia. Then, they are entered into the library's inventory system, stored, and ultimately are purged in accordance with state retention periods for each type of document. The library is paid a fee per box for providing the storage in a climate-controlled atmosphere, and collects a small fee to retrieve the records for the agency.

At Purdue, which has more than 68,000 students and approximately 17,800 faculty and staff, a vast amount of data is generated, and document retention responsibilities often fall to the department level. "Each type of document should list a contact name — someone to whom staff can turn if they have a question about retention and/or disposal," Fish explains.

## **ENFORCEMENT**

One challenge at 3M, says Martínez, is ensuring that every subsidiary in the world complies with the company's document retention policy. "Generally, all countries have specific legal requirements related to years of retention, so our policy clearly establishes what the retention period should be in accordance with the company policy or local applicable law, whichever calls for a longer retention period."

Enforcement should be an ongoing process. "The concern to me," says Fish, "is constantly making sure that folks are paying attention to the document retention policy, and that they're evaluating and updating it as necessary. There is a need to look at things constantly, in an ever-changing environment, to make sure the policy doesn't get outdated."

Policies should address destruction, but the trick is ensuring that disposal rules are followed, a particularly difficult task in larger organizations. "You should have some kind of a trigger so when you hit the end of that retention period, you dispose of those documents," Fish says.

Ensuring compliance should begin with the creation of a document enforcement team. "They should come from across departments," says Lange, "not only from the litigation department, but from information technology all the way up to someone from your executive team. The team should own and follow the document retention policy and make sure that once litigation ensues, document destruction is halted immediately."

## **PRIVACY CONSIDERATIONS**


One of the greatest challenges, says Crispens, is ensuring the confidentiality of a customer's or an individual's private information, such as payroll or tax records. The Library of Virginia, which oversees document retention of state agencies, determined that destruction of confidential or privacy-protected records typically will be shredded by state agency officials. "Deletion" of confidential or privacy-protected information in computer files or other electronic storage media is not acceptable. Electronic records must be "wiped clean" or the storage media physically destroyed, according to the policy. "Essentially, the stored records that are marked as needing privacy protection are shredded at expiration," says Crispens. "In the interim, only certain designated people could retrieve the confidential record storage box if the information was needed."

In terms of privacy in the workplace, the issue varies from country to country. In the United States, privacy laws have little impact in the workplace. A Pennsylvania court, for example, in *Smyth v. The Pillsbury Co.*, held that an employee could not base a wrongful discharge claim on right to privacy because he had no reasonable expectation of privacy in e-mail communication over a company system.

"That lack of expectation of privacy gives corporations a broad brushstroke when it comes to preserving evidence and documents," says Lange. "It means that if they need to take an image of your computer for litigation, they're going to get the e-mails you send to your family. In other countries it's not as broad. There is a higher expectation of privacy, and corporations don't have the right to dig into e-mail that might be personal."

## **INTERNAL AUDITING'S ROLE**

"Internal auditors play a huge role in making sure that a corporation is following its document retention policy and that when required, the policy's destruction ends at the appropriate time," says Lange. "But I don't think it's something that internal auditors can do on their own. They need corporate buy-in at every level of the organization."



Martínez says efficient management of records ultimately provides internal auditors with the crucial knowledge needed to evaluate a company's internal control effectiveness. "A well designed document retention policy can provide us many benefits: improved efficiency on the management of active and inactive filings, less departmental demand to purchase filing equipment, and improved security against unauthorized access of internal and external parties."

To read the general records retention and disposition schedules for Virginia state agencies, visit The Library of Virginia's Web site, [www.lva.lib.va.us/whatwedo/records/sched\\_state/index.htm](http://www.lva.lib.va.us/whatwedo/records/sched_state/index.htm).

The Institute of Internal Auditors · 247 Maitland Avenue · Altamonte Springs, Florida 32701-4201 U.S.A. ·  
+ 1-407-937-1100

[www.theiia.org](http://www.theiia.org) All contents of this Web site, except where expressly stated, are the copyrighted property of The Institute of Internal Auditors, Inc. (The IIA®). [Privacy Policy](#)

Reprinted with permission from Auditwire, March/April issue, published by The Institute of Internal Auditors Inc., [www.theiia.org](http://www.theiia.org).