

A Brave New World

At the Core

This article:

- Provides examples of prudent document destruction programs
- Offers advice on how to destroy records properly and legally
- Discusses tips for selecting a destruction contractor

Proper and prudent document destruction is as important as any other milestone in a record's life cycle

Records and information destruction activities have shocked and captivated audiences over the past year. The sometimes heated discussion has been driven largely by divergent perspectives and has resulted to some degree in mixed messages and confusion about the propriety of information destruction. On the other hand, legislation such as Gramm-Leach-Bliley and Health Insurance Portability and Accountability Act (HIPAA) are forcing the issue of information destruction on the financial and healthcare worlds.

Willie Geiser and Bob Johnson

States such as Wisconsin, California, and, most recently, Georgia, have passed laws to fight the rising wave of identity theft, requiring businesses to destroy obsolete personal information. Shredding, however, continues to be characterized in the media and by some politicians as an inherently dubious, even suspicious, activity with no purpose other than to conceal incriminating information.

The fact is that proper, scheduled destruction of information is both a highly responsible and necessary business activity, one mandated by legal and regulatory requirements – as well as

common sense – to protect consumers and businesses alike. Proper and prudent document destruction is as important as any other milestone in the life cycle of a record.

A Rose is a Rose (Even in the Wastebasket)

It is understandable that many records and information managers primarily focus on the paper-based and electronic records that are conveniently stored on shelves or disks for a required (and, hopefully, specific) period of time. The task of managing records kept for legal,

regulatory, and business purposes is, however, increasingly daunting. Maintaining those records in a rationalized, centralized, and organized manner is crucial to compliance, retrieval, retention, and disposition. Add to that the furious pace at which technology affects records creation, access, and distribution while satisfying the demands of internal customers, and it is easy to see why the resources, time, and attention of records managers are already stretched thin.

In such an environment, some functions will get less attention than others. For example, record managers have given up their influence on a significant segment of records: incidental records, which are sometimes called non-records. As defined in Chapter 44, U.S. Code, 3301, incidental records include extra copies (e.g., photocopies) of documents such as routing slips, transmittal sheets, materials made for museum purposes, and intermediate drafts, created or received throughout the course of the day, that have no value beyond their immediate use. They can comprise as much as 60 percent of the waste generated in an office environment. These records may have a life of a few minutes or a few weeks, but often they are discarded without any acknowledgement of their creation or a policy regarding their proper retention and disposal.

Do these incidental records have importance? How often has the “smoking gun” turned out to be a handwritten note to a colleague? There have been lawsuits in which simple drawings on cocktail napkins were admitted as significant material evidence. (A well-known incident involves a multimillion-dollar settlement in 1973 in which John Atanasoff, a professor at Iowa State University, produced a cocktail napkin that proved that he was the originator of the computer in 1937.) A discarded Post-it Note® could prove as much a bona-fide business record as correspondence from the CEO to the Securities Exchange Commission.

Reclaiming Turf and Missed Opportunity

Right or wrong, the status and value (and longevity) of individuals within corporate America often is determined by internal spheres of influence. Records managers who have relinquished control over incidental business records to the facilities manager, an offsite storage company, or a janitorial service as a



The Federal Bureau of Investigation (FBI) estimates that U.S. businesses lose tens of billions of dollars every year due to the theft of their information.

waste-disposal issue are missing an opportunity to show their value and, more importantly, to properly execute their responsibility and serve their organization.

The Role of Destruction in RIM

There are many reasons organizations would be well advised to make sure they routinely destroy discarded original, duplicate, and incidental records in an organized and documented method. All of those reasons focus on protecting the organization.

Dumpster Diving

It is obvious that discarded records should not fall into the hands of com-

petitors. The risk of this occurring depends upon circumstances particular to the facilities and situation. As with any risk analysis, the severity of the consequences resulting from the occurrence needs to be considered. The marginal cost of knowing that all information is properly destroyed is minimal compared to the potential resulting damage, so this should be an easy decision to make.

There are some facts that may help put the decision and risk in perspective. The Federal Bureau of Investigation (FBI) estimates that U.S. businesses lose tens of billions of dollars every year due to the theft of their information. Nine out of 10 large companies have employees dedicated solely to the competitive intelligence function.

As recently reported by Ameet Sachdev in the *Chicago Tribune*, contractors hired by a large consumer-products firm were caught in the midst of a six-month Dumpster-diving campaign at a rival's headquarters. One industrial intelligence professional commenting on the incident claimed to have hit more than 2,500 Dumpsters in the pursuit of corporate information on behalf of clients. Partly because most victims of Dumpster diving never know they have been victimized, these professionals consider the wastebasket (or Dumpster) to be the single most available source of competitive corporate information.

Identity theft is another increasing risk from casually discarding information. The epidemic of identity theft and the publicity that has surrounded it has elevated the issue of privacy protection to one of the most pressing consumer-rights issues. Public sentiment on this matter is at the core of HIPAA, Gramm-Leach-Bliley, and the myriad of state laws mandating personal information protection. Casually discarded information can be, at a minimum, embarrassing and costly for individuals and organizations. Violations of the laws regarding privacy may carry criminal liability, but that is little consolation to victims.

Use It or Lose It

Any reasonable person understands the devastating results of information falling into the hands of a criminal, competitor, or reporter. But there is a more subtle and potentially more insidious ramification from casually discarding confidential information. An organization actually could forfeit the right to defend its trade secrets, proprietary technology, and non-competition agreements if it fails to protect that information at every point.

The precedent for this penalty was set in the late 1950s. A Detroit-based company, Cadillac-Gage, was in the midst of a booming business manufacturing armored vehicles for transporting currency and valuables. A group of high-level executives left the firm and set up shop in Florida to compete in the armored vehicle manufacturing business.

Cadillac-Gage immediately sued the new company for stealing trade secrets, including customer lists, proprietary engineering documents, and design information. The defendants' attorney successfully admitted evidence that he had retrieved from Cadillac-Gage's trash, including customer lists and schematics. He effectively argued that Cadillac-Gage was not protecting the very information it was claiming was so vital and that it was asking the courts to protect.

As a result, the judge ruled against Cadillac-Gage. He determined that what is claimed as trade information must be protected in order for those rights to be recognized by the court. This case has been cited hundreds of times since, including in the 1987 U.S. Supreme Court case *California v. Greenwood*, in which the justices ruled in a split decision that all rights to ownership and expectations of protection are forfeited when something is casually discarded. It also was ruled that it is not illegal to take something once it is discarded. This means that there is no such thing as "stealing" from a Dumpster.

Another protection that is forfeited by casually discarding information is that afforded by the Economic

Espionage Act (EEA) of 1996. Before the EEA, organizations were responsible for exercising on their own their trade information protection rights in court. They were forced to bring suit against anyone they accused of violating their rights. However, the EEA changed that. It is now a federal offense to violate another organization's trade information protections. The fines can go as high as \$10 million and may include 15

years in prison. If the Department of Justice chooses to pursue the case, it – rather than the corporate entity – will bring the charges and prosecute the violators at the government's expense.

So the EEA heralds a landmark of protection for corporate America whereby the federal government itself will protect trade information and severely punish the culprits. The only impediment is that the organization victimized by the trade

information violation must be able to prove that it took all reasonable measures to identify and protect that information. By failing to put in place effective comprehensive procedures to destroy all discarded information, an organization virtually guarantees that the EEA will not protect them.

An interesting measure of an organization's information security program is the degree to which employees are exposed to information. Essentially, employees should have access to corporate information on a need-to-know basis. Widely dispersing or exposing information to employees represents a security hole that also can jeopardize trade information rights protection. This concern is one of the reasons that security collection containers are replacing wastebaskets. It is neither realistic nor reasonable to claim that information is being given requisite security when it is deposited in open trash cans. It is also one of the many reasons that contract information destruction services have come to be the most prevalent resources for records disposal.

Doing It Right

Given that destruction is now a required, or at least prudent, milestone in the life of any record and given that auditors, prosecutors, litigants, the media and, unfortunately, the general public sometimes mistakenly perceive it to be inherently deceitful, it is important to structure destruction policies and procedures to minimize even the appearance of impropriety. The two

most important components that can eliminate any chance that destruction processes will be perceived as inappropriate or nefarious are *consistency* and *documentation*.

Consistency

1. Be consistent in what is destroyed. Never destroy one class of records or type of media while not destroying another. This is important not only for appearance's sake but also to establish due diligence in protecting the organization's trade information and client personal data.
2. Be consistent about the method and means of destruction. If an organization has a regular method of destruction, any destruction outside that procedure draws attention and risks the appearance of impropriety. Being consistent about the method of destruction between classes of records and media is also important for the same reason.
3. Be consistent in the procedures used for destruction in decentralized operations and from department to department.
4. Be consistent regarding the timing by which records are destroyed.

For instance:

- Incidental records comprising the daily waste stream are collected in secure containers and destroyed weekly.
- Duplicate records squirreled away in office drawers, reading files, and

chronological files are collected and destroyed quarterly.

- Original stored records that reach their retention period are destroyed semi-annually.

Documentation

1. Document all destruction policies and schedules, covering all classes of records, and describe acceptable collection and destruction methods.
2. Document the training of employees regarding the organization's information protection and destruction policies.
3. Document subcontractors' and vendors' awareness of or instruction about the company's policies on protecting trade information and personal data. It is not uncommon for large firms to have good information protection programs, while vendors and subcontractors casually discard records and thereby compromise the internal destruction program.
4. If a contractor is used for destruction, document the criteria by which it should be evaluated and selected. Also, document the actual process of selecting the contractor.
5. Document every instance of information destruction.
6. Maintain internal and contractor destruction activity records permanently.

Consistency and documentation are the only ways to achieve the transparency necessary to eliminate any hint of subterfuge.

The World of Contract Destruction Services

The National Association for Information Destruction (NAID) estimates that there are approximately 600 companies in the United States offering records destruction services. They include dedicated service providers who do nothing but information destruction as well as record storage companies and recycling companies.

Document Destruction Education

All the National Association for Information Destruction's (NAID) member companies – currently 240 – subscribe to a strict written code of ethics. Recently, the non-profit trade organization went one step further by introducing the NAID Certification Program (www.naidonline.org/certified_members.html). NAID members seeking certification submit to an annual audit by third-party security consultants to determine whether or not they meet NAID's specific standards. The NAID Certification has completed its second year and has helped hundreds of customer organizations select a destruction vendor.

As one might expect to see in such a rapidly growing industry, especially an unregulated industry with participants from many business models (i.e., shredding, recycling, storage), the security and procedures employed by information destruction service providers can vary widely. The problem with such variations is that organizations can never really completely hand over their obligation to protect their information. The degree to which an organization is really protected by using an information destruction service has as much to do with the diligence put into the selection of the vendor as it does with the potential damage caused by the information surfacing after the fact. In other words, if XYZ's records were to surface and cause a problem after having been transferred to a destruction contractor, XYZ's negligence could turn as much on the process they used to hire the contractor as the damage caused by the resulting breach.

In selecting a destruction contractor, several things should be verified as part of the thoroughness of the process.

1. Make sure the service provider is not subcontracting the destruction service and has the ability to provide the destruction with no transfer of custody. If destruction services are provided by a company primarily offering records storage or recycling, do not assume those services are being rendered first hand. No one but the records' primary owner should decide which contractor actually provides destruction services.
2. The destruction contractor should screen employees through background checks at the time of hiring.
3. Threshold levels of insurance should be required and verified.
4. The particle size of the materials resulting from the destruction process should be verified to meet procedural minimums.
5. If plant-based service is used, verify that access is restricted to operational employees.

6. The contractor's service employees should be easily recognizable and identifiable.
7. The contractor should provide documentation after the fact, establishing the date that the information ceased to exist, where it was destroyed, and how it was destroyed.
8. The destruction contractor should provide documentation upon receipt of the materials to be destroyed that acknowledges and accepts fiduciary responsibility for the confidentiality and destruction of the materials.

Implementing Standards

With increasing pressure for organizations to protect sensitive information, it is understandable that some would look for what might appear to be the least-expensive alternative to accomplish the task. And, of course, there will always be someone to tell them what they want to hear.

Landfilling and recycling are most often offered as an inexpensive alternative to destruction, and proponents of those methods confidently plead their case. What seems to be the most convincing selling point of using landfilling as a destruction alternative is when the landfill operator promises to dig a special hole strictly dedicated to receiving the sensitive material. Upon the dumping of the records in the hole, the landfill operator then immediately buries the material.

The truth of the matter is that this misses the mark in the most basic sense; the media containing the information is still intact, readable, and retrievable. And, of course, many landfills are not holes but hills. A study conducted by the University of Arizona established that the act of burying documents in a landfill effectively preserves them. Not only will the information be around longer than if it were left in the sun and air, but also it will be identifiable when unearthed and, most importantly, potentially subject to legal discovery. Technically and legally, with the information still existing intact, it is conceivable that during legal discovery the

records would have to be unearthed and produced by the defendant – however inconvenient and costly.

Recycling is sometimes represented by vendors and accepted by consumers as an alternative to the destruction of paper records. However, sending office paper to a local recycler with no intention of shredding it is far from being reasonably passable as prudent destruction. The paper may be sorted, for example, by unscreened employees to maximize value. Paper unacceptable because of type or color is often discarded. There is no way to determine when the materials were actually destroyed (when they cease to exist). Furthermore, there is no acknowledgement of fiduciary responsibility. At the other end of the process, the paper mill usually stores the bales of intact paper outside for weeks or months. It is estimated that some 10 percent of the paper is contaminated or deteriorated and summarily discarded intact by paper mills. In short, selection of this process will not meet the most basic elements needed to establish that care was exercised.

A reasonable-sounding scenario for recycling paper documents involves truckloads of records being hauled directly from storage to the paper mill. Here, however, the requirements recommended earlier regarding the selection of a destruction vendor are still not met.

The Ultimate Litmus Test

To test how confident records managers are about their records destruction program, all they have to do is imagine themselves in a deposition.

- “What method did you use to select your destruction contractor?”
- “Did the company have written policies and procedures for employees covering the disposal of all classes and categories of records?”
- “What about the incidental records discarded in the daily trash?”
- “Why did you pick last October to conduct a major purge and destruction of records?”

How well records managers fare in such a mock deposition depends upon how well they have executed their responsibilities. Not confronting these issues is to ignore one of the most significant responsibilities of managing an

organization’s records according to the life-cycle model. Then it is almost inevitable that at some point records destruction policies and procedures will surely be challenged at some level, internally or externally. ■

Willie Geiser is owner and president of All-Shred Services, and is currently President of NAID. He may be contacted at wgeiser@allshredservices.com.

Robert Johnson is the founder and Executive Director of NAID. He may be contacted at exedir@naidonline.org.

References

- Lavelle, Louis. “The Case of the Corporate Spy.” *Business Week Online*. 26 November 2001.
- Sachdev, Ameet. “P&G Admits Unilever Garbage Search – Regrets Voiced by Spying on Hair Care Unit.” *Chicago Tribune*. 1 September 2002.
- “Supply of and Recycling Demand for Office Wastepaper, 1990 to 1995.” Available at www.mdrecycles.org/Guide/officerecyclingmain.htm (accessed 7 October 2002).
- “There Are No Secrets.” *Venture Magazine*. February 1988.

READ MORE ABOUT IT

Hill, Lisa B. and J. Michael Pemberton. “Information Security: An Overview and Resource Guide for Information Managers.” *Records Management Quarterly*. January 1995.