

# Processor: Data Deletion Processes & Standards

By: Elizabeth Millard, January 14, 2011

<http://www.processor.com/editorial/article.asp?article=articles/P3301/32p01/32p01.asp&guid=>

Even with widespread awareness of data storage and data deletion practices, the numbers from a recent Kroll Ontrack survey are eye-opening. The information management firm found that of the 49% of businesses that are systematically deploying a data erasure method, 75% don't delete data securely, leaving them susceptible to data breaches.

Only 19% of those surveyed use data deletion software and even fewer, 6%, use a degausser to erase media. When asked if and how businesses verify that data has been deleted, 16% noted that they rely on a product or service for confirmation, but 22% simply reboot the drive and look to see if data is still there.

"The survey results don't surprise me at all," notes Jeff Pederson, manager of Ontrack Data Recovery operations at Kroll Ontrack ([www.krollontrack.com](http://www.krollontrack.com)). "A lot of people believe their data is erased, but they don't have a way to check that's very effective. Or they don't have a system in place that really works. This is a challenge for many enterprises, and it's putting them at risk."

## ■ Major Problem

At a former employer, Pederson found that the IT department often tried to repurpose machines as soon as an employee had left. This can be a major issue, because if that person is involved in any litigation with the company, the data involved needs to be saved until those issues are resolved. These "litigation holds" are very common, and an enterprise that deletes data when one is in place could face significant penalties.

In general, the larger issue with data deletion seems to be cost, Pederson has found. Because wiping a hard drive clean and rebuilding it takes more time than simply deleting a hard drive's files, many IT departments take that shorter route. "The problem with that method is that there's still tons of data on that computer," Pederson says.

To combat the issue, some companies simply store all their data for as long as possible, but that's a poor solution, as well, because there are regulations and mandates in place regarding data destruction timeframes.

"The reason for doing proper data deletion is because it reduces your e-discovery costs," says Pederson. "If you're not destroying data, you will definitely have a problem at some point." For example, a lawsuit might ask for all emails related to a certain product. Instead of having 100 messages that stretch back during the usual storage time period of two years, a company might have 10,000 messages over the last decade. Because those emails are related to the case, the company would have to pay someone to go through them and classify each message in terms of relevance.

## Key Points

- Perceived cost is usually the main factor for a lack of data deletion processes and standards.
- Create a data deletion process based on the type of data involved and industry regulations.
- Set up hardware and software tools that can help categorize data and be used for deletion; manual deletion strategies simply don't work, given the amount of data involved.

“If you have thousands of documents or emails that you don’t need to be saving, you may be risking a situation in the future that will waste a huge amount of time and money,” Pederson says.

### ■ Create A Policy

Determining data deletion timeframes depends largely on the type of data in question and the industry involved. For instance, tax data is regulated by the federal tax code, which notes that all records must be kept for seven years. That law cuts across all industries, but other regulations, such as HIPAA, affect healthcare organizations and the vendors that serve them.

“With HIPAA and some other privacy laws, the law states that you can only keep data for a certain amount of time and then you have to delete it,” says Pederson. “Some companies that get hacked get into even more trouble if they have data that goes back too far. You can’t just save everything and keep spending money on storage. You have to know the relevant laws on the types of data in your system.”

Another part of the policy is to identify data that doesn’t need to be stored, adds Pat Midden, an associate at law firm Oppenheimer, Wolff & Donnelly ([www.oppenheimer.com](http://www.oppenheimer.com)). “Ask yourself why you need a particular kind of data,” he advises. “For example, if you’re capturing Social Security numbers and they’re not relevant to your business, then don’t save them. Think about what information you really need to store.”

### ■ Fill The Tool Box

To fulfill the mandates set in the policy, it’s imperative to find hardware and software products that work well with a company’s systems. Simply asking employees to prioritize emails and do data deletion work isn’t going to address the issue, Pederson notes.

“You just can’t go through 500 emails a day and try to categorize them,” he says. “As a result, so many people that I’ve met are digital hoarders. They simply create subfolders and throw stuff in there. I’m a firm believer that you need some kind of technological tool.”

\*\*\*