

E-Discovery: Saving by Not Saving

By: Carrie Mallen

December 2010

California Lawyer

<http://www.callawyer.com/story.cfm?pubdt=NaN&eid=912901&evid=1>

For decades, corporations have been admonished to save, copy, "binderize," back up, and store as much information as they can. But in the age of e-discovery, this outdated practice is costing Corporate America billions of dollars. In the past decade alone, corporate legal expenses have increased by more than 75 percent, and the annual expenditure per company clocks in around \$1 million, according to the 2010 Fourth Annual ESI Trends Report by Kroll Ontrack.

Kroll's survey of 203 in-house attorneys and IT professionals also noted that although more than half of the companies surveyed had an e-discovery strategy, only one-third had tested it. Furthermore, respondents for 55 percent of the companies either said their policies hadn't been updated to accommodate new technology and social media, or didn't know.

But at the heart of the upward swing in litigation costs is the irresistible tendency to blindly save everything that comes across the electronic transom. Indeed, e-discovery costs are tied directly to the volume of data. But data hoarding also increases legal risk. In the time since the Federal Rules of Civil Procedure were revised in 2006 to address electronically stored information (ESI), a fair amount of the material produced in litigation arguably was not subject to retention requirements. Rather, it became part of litigation for the worst possible reason: because it existed—in vast amounts. Companies—and in-house counsel—should know that they can cut litigation costs if corporations adopt practices that resist the urge to save unnecessary data. Consider these steps.

Embrace Technology

Data that has no business value and is unrelated to governmental regulatory obligations should be purged according to a well-articulated and routinely enforced corporate records retention policy. But don't rely on employees to perform this crucial task: They could inadvertently introduce errors. A records management software program can automate retention and purging and accommodate litigation hold requirements. Given the array of technology that's available, select a program according to the company's regulatory and business needs.

Assemble a Task Force

To get a handle on the ESI that may be lurking in warehouses, servers, or individual computers, engage a task force made up of representatives from IT, legal, and business departments in every unit across the enterprise. Identify extraneous data, and determine whether that data is subject to a legal hold or regulatory retention, or relevant to ongoing business. If not, dispose of it according to company policy. In the process of identifying unnecessary data, the ESI task force will also naturally identify potential logistical and communication problems—and best practices—for retaining and disposing of data. Cultivate institutional memory by documenting the decisions and policies that emerge from the task force.

Create a Data Map

Data maps outline a company's data systems so that potential sources of ESI can be quickly identified, and they're necessary to comply with disclosure obligations under Rule 26 of the Federal Rules of Civil Procedure. The ESI task force can begin to draft a data map that will ensure that all corporate information is accounted for; the riskiest ESI is the unstructured data on unmapped servers, and the forgotten storeroom of server tapes or the legacy data on old computers.

Aside from litigation, data maps become critical when a company is acquiring new business units in various industries. Without a data map, it is difficult to integrate the retention policies of the new unit with existing ones, particularly if the acquired company operates in an industry with different regulatory requirements. As part of the due-diligence performed during acquisitions, ask for a data map from the target company.

Secure Executive Support

Hoarders exist across all business functions, so proactive measures to mitigate risk must come from the top. Companies should consider corporate culture and employee work habits in creating policies that will prevent risky data from lingering on laptops or home computers following off-site work. This makes top-down advocacy of these policies crucial. Executives can consider capping the amount of data allowed in email inboxes, prohibiting data storage on local computer drives, and locking down USB ports.

There are many ways to create a cost-efficient e-discovery program, but success hinges on effective implementation—and curtailng the entrenched habit of hoarding all that electronic data.