

Stephen Whetstone,
an attorney and
vice president of
client development
and strategy with
Stratify, an Iron
Mountain company



ACCURATE RESULTS AT A FRACTION OF THE COST

Knowing What You Have is the Key to Preparedness

By Paul Desmond

Photograph by Tim Llewellyn

EVER-GROWING VOLUMES OF DATA PRESENT MYRIAD challenges for IT departments, from how to store it to how to back it up. But one challenge in particular that gets scant attention is how to deal with data should your company become involved in litigation.

Even organizations that have considered their litigation readiness aren't always sure which data must be retained, or for how long. Unfortunately, the answer is often "it depends"—on the appropriate regulatory requirements, who created the data and when, what it pertains to, and whether litigation is pending that may relate to it. Then there are business needs—how long the data must be retained for disaster recovery purposes, what is its intrinsic value (for intellectual property purposes or otherwise), and what it costs to store it.

What is clear, however, is that ignoring litigation readiness is not an option. A high-profile case can rack up millions in fees as lawyers search for relevant data—assuming that data still exists. If it's been deleted or you can't produce it, your organization may be subject to huge fines and worse, damage to your brand.

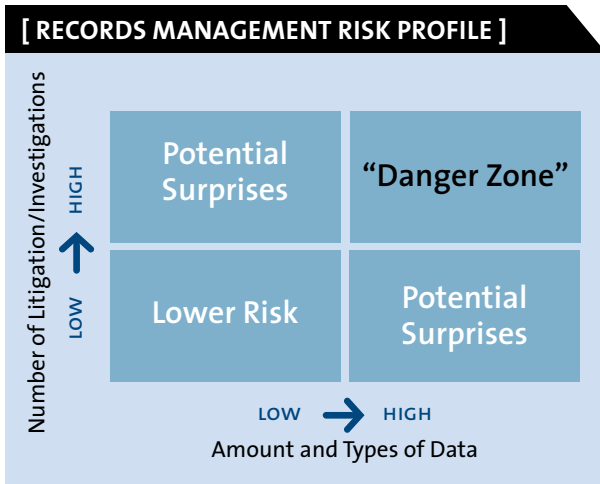
Proper planning will help you avoid such scenarios. That means putting in place a records management plan that takes into account litigation readiness and ongoing business needs. The plan also should outline the steps to take in the event you need to institute a litigation hold—the point at which you must start preserving data that may be relevant for litigation—and the technical steps required to find the preserved data, including the use of automated tools.

BOTTOM LINE
High-profile litigation can cost your company more than money if you can't produce the data that the courts demand. Protect yourself by implementing a comprehensive records management plan before trouble arises.

Outlining the Risks

A study last year by the research firm IDC predicted that in 2010 there will be more bits of data than grains of sand on all the beaches in the world. While much of that data will be generated by consumers, about 60 percent of it will cross corporate networks. Another research firm, Radicati, estimates each corporate worker generates 4.3 gigabytes of data per year.

In addition, courts are still feeling their way through the amended Federal Rules of Civil Procedure on electronic discovery that took effect in December 2006. Previously, there had been no changes to those rules since 1970, despite the extraordinary advances in technology and prevalent use of electronic information, says Stephen Whetstone, an attorney who is now vice president of client development and strategy with Stratify, an Iron Mountain company.



Among other significant changes, the amended rules define in great detail what kinds of electronically stored information must be preserved, including, in some cases, various types of hidden metadata and embedded file data. In essence, the rules heighten the overall litigation risk environment and make it imperative that all companies have a comprehensive records retention policy in place—and one that is defensible in court.

While the federal electronic discovery rules apply only to federal court proceedings, state courts often track their federal counterparts for discovery purposes. Moreover, matters that involve government agencies or criminal complaints can demand even more stringent data management. For example, data from backup tapes usually is not discoverable under the FRCP because it is “not reasonably accessible” data, Whetstone says. But the Securities and Exchange Commission is not bound by that distinction and can demand that a company turn over all data related to an investigation, wherever it resides.

Should your company become embroiled in litigation, the cost of finding and producing the required data can rapidly escalate. The traditional approach is to hire an army of lawyers who use keywords and Boolean searches to review your corporate data for relevant documents. At an average billable rate of \$100 an hour—which is enough time to get about 60 documents reviewed—a company can run up a substantial bill.

What’s more, the accuracy of such an approach is questionable at best. “Several studies have shown that manual review by lawyers using keywords, Boolean and other traditional search technologies may be only about 25 percent to 50 percent accurate,” Whetstone says. “That means you may miss more than you find, which has significant implications.”

Should you fail to produce documents the court deems relevant, whether because the data no longer exists or you simply couldn’t find it, the penalties can be severe.

A jury assessed \$1.45 billion in damages, \$800 million of which were punitive damages, to Morgan Stanley after the judge instructed jurors to assume that the data the defendant company failed to produce was damaging to its case. While that verdict was overturned some 18 months later, the damage to Morgan Stanley’s reputation was done. An ongoing antitrust case involving Intel and AMD has seen a high-profile technology company repeatedly brought into court over accusations that Intel failed to lock down data when the litigation first began. No matter how the case turns out, it may well harm the company’s reputation.

Preparing Your Plan

You can avoid that kind of monetary damage and unfavorable press by developing a records management plan long before there are any whispers of litigation.

The first step is to assemble a team that will devise and implement the plan. The team should include:

- IT personnel, who will be instrumental in implementing the technical aspects of the plan
- Corporate counsel, to provide legal guidance
- Compliance personnel, to offer input on the regulations that must be considered
- Business executives, who can assess how the plan will affect day-to-day business and provide the executive support and direction crucial to its success

The next step is to conduct a risk assessment. The goal here is to determine how likely your company is to be involved in litigation. That will determine what kind of document retention policies you need.

Whetstone advises companies to consider using a familiar quadrant grid to determine risk. (see table above) Which quadrant your company falls into will affect how you implement a records management plan. Companies that fall into the upper-right quadrant (those in highly regulated industries that are likely to be subject to complaints and have lots of distributed data of various types) are at high risk and will need a stringent policy.

Then prioritize your data. Assign the highest priority to retaining data generated by C-level executives and work down from there. Keep in mind that prioritizing data is a gradual process that will take time. When determining what to classify, keep your industry in mind and follow whatever specific regulations you are subject to.

Putting the Policy in Place

Of course, any policy must be enforced throughout the enterprise, and that starts with support from the proper authorities. For records management, that means you need buy-in—and funding—from top management.

Once the policy is in place, it’s incumbent on IT to maintain accurate records management logs and routinely audit the system. This will help you determine whether

the policy is working and point the way to any necessary adjustments.

It's also important to follow your records management plan religiously. If you can't produce certain documents—even under subpoena—you may be protected against penalties if you can prove that you've been following your records management policy.

“At the end of the day, the law doesn't require perfection, but it does require a good faith, reasonable effort to fulfill your obligations,” Whetstone says. “If information is lost as a result of routine IT operations, a company may find protection under the Federal Rules of Civil Procedure's ‘Safe Harbor’ provision. But the loss must be in good faith—companies cannot willfully or blindly ignore their obligations to preserve relevant data or fail to suspend document destruction policies in the face of litigation. That won't work.”

Once a litigation hold kicks in, you are expected to suspend or amend your routine records management processes for data that may be relevant. Corporate counsel—not IT—should make that call on relevancy, and IT and records management should be ready to comply with a hold request.

You'll likewise have to craft a defensible data-gathering plan that can be implemented relatively quickly. In most cases, parties in litigation have 99 days or less to confer

about what data must be preserved and to produce it.

Electronic discovery tools can bring accuracy and speed to the discovery process. Stratify, for example, has tools that compare every file that has been preserved to every other, then groups them in virtual folders. “So lawyers can say, ‘This is all spam, this is marketing data, and here are the technical documents that I really care about,’” Whetstone explains. “You get through it more quickly and accurately. We've created order out of chaos.”

With no end in sight to the exploding volumes of data, and with the threat of litigation a fact of corporate life, companies must take steps to protect themselves. Putting in place a sound, legally defensible records management policy and ensuring employee compliance are crucial no matter which side of the legal battle you may be on.

But even the best policy won't fully insulate you from the time and costs associated with the discovery process should litigation arise. You will almost certainly need help sorting through all of your data. Using tools like those offered by Stratify can help you quickly classify your data, enabling the lawyers to focus their efforts on the documents that are most relevant to your case. You'll get more accurate results at a fraction of the cost. ▲

PAUL DESMOND IS A FREELANCE TECHNOLOGY WRITER
BASED IN MASSACHUSETTS

[CHECKLIST FOR LITIGATION READINESS]

HERE ARE SOME GUIDELINES FOR establishing a litigation-ready records management plan.

- Define what constitutes an official business record in your organization. A personal email from a customer service representative? Probably no. Email from the CEO that pertains to sensitive negotiations? Probably yes. Additionally, the policy needs to define how long you'll keep each type of business record.
- Determine how you will store and back up various data types. One size does not fit all. Different file types require different storage techniques and periods. Some records must be kept for prescribed periods of time. You must understand the appropriate laws and draft your plan accordingly
- Carefully craft the policy. Your plan must be clear, practical, repeatable and defensible. Strive to create policies that don't rely too much on human intervention. Content management tools can automatically classify documents based on predefined keywords and phrases, without requiring individuals to make document-by-document decisions or, in some instances, any decisions at all.
- Distribute the policy to all employees. They should be required to acknowledge receipt and indicate that they understand it. Doing so can protect you from instances where a rogue employee knowingly violates the policy, then claims he never knew it existed.
- Include a “go live” date. Make this at least a few months in the future to avoid the perception that you put the policy in place quickly because of anticipated litigation. Otherwise, it may be hard to explain why you destroyed relevant data on the eve of the receipt of a subpoena or complaint even if you had no knowledge of the pending claims.
- Appoint an owner. One person should be responsible for records management and for determining when a litigation hold should take place. Publish that person's name throughout the organization to eliminate any confusion over who has the authority to order information be locked down.