

Are You too Small for an Email Retention and Archiving Policy?

Joel Snyder, Contributor
03.15.2010

Short answer: No. Why? Because sooner or later, you're going to be involved in a dispute with some other company. Maybe it's about money; maybe it's about goods that don't meet expectations; maybe it's about employment matters; maybe they just don't like the look of your logo. It's going to happen, and if your company is more than a year old, it probably already has -- maybe many times. If it enters the court system, you'll enter discovery procedures, and I can guarantee you the other side is going to ask to see your email.

In this tip, we'll review how organizations, both large and small, should prepare their email retention and archiving policy.

Rule changes

In late 2006, the [Federal Rules for Civil Procedure](#) changed -- or were clarified, if you prefer -- and "electronically stored information" was swept directly into the realm of discovery. You can learn about the details of these changes elsewhere, but there are three key points you need to know:

1. Discovery will almost always involve electronic records, starting with email and continuing to any other documents that you have stored electronically.
2. If you don't have the electronic records, and you should, then you can lose your lawsuit for that reason alone.
3. A judge gets to decide whether your records are "reasonably accessible" or not, not you.

Keeping electronic records

Let's go through these three points, because small businesses need to know about them as much as large ones.

First, is the question of electronic records. The courts understand that most of our records are electronic, and so they expect you to save them and make them accessible in the same way that you would have kept paper records in the past. Email is the biggest deal here because trial lawyers have found that email leads to wonderful insight into what a company was really thinking and saying inside.

The problem is that most of us in technology think of email the way we do a phone call: ephemeral, short-term, fairly personal and of low importance. You have to change that mindset because email is now given the importance of a memo. That doesn't mean intensive re-education, but it does mean that everyone in the company has to understand that their private email may not be private during a stressful period for the organization.

Second is the question of keeping records. If you're huge, then you're covered by external regulatory rules, such as Sarbanes-Oxley, which mandates email retention periods. If you're small,

you have to make up your own policy, and you have to enforce it. Why? Because only with a policy can you set boundaries for what someone else can ask for during discovery.

It doesn't really matter what your policy is. In other words, the Federal rules don't give a lot of guidelines, but your policy should be one that makes sense for your industry and your company size. Your policy should cover the basics of how you classify records and what the policy is for each type of record. When people ask me for advice, I usually suggest making the electronic policy match up with what you've been doing for physical paper records all along. That gives you a good framework to start with, and also is very defensible in case anyone questions your policy.

For example, you would include business email as part of your policy. You may say that email is saved for 3 years, or 30 days, or anything you come up with. What is important is that you write it down and then enforce it by regularly destroying records that should be, by policy, destroyed. However, there is a huge caveat here: Once your company reasonably believes that there will be a court action, it must stop destroying records. Don't wait for a court order or a trial to begin -- as soon as you get wind of a potential legal action, you have to stop deleting old data. There is a safe harbor if you genuinely lost the records, but there's no quicker way to lose a lawsuit than to say: "Oh, we forgot to turn off the deleting program for our email."

Third is the question of reasonable accessibility. Some IT folks have hidden, in the past, behind a pile of backup tapes with the claim that production of old email is hard, expensive and time consuming. That won't fly, and you can also be knocked out of court if you cannot produce information that a judge thinks should be reasonably accessible in a timely way.

In other words, we are now being required to build processes into our IT infrastructure that allows us to get documents and records out quickly and efficiently. I can't tell you what you need to do this, because every company is different. You can buy a low-end archiving appliance or you could even just CC: every single message to a mailbox that is cleaned out according to a rigid schedule. Some folks don't like these approaches because they lose metadata, such as whether the recipient even read the message or when they replied, but you will find that small businesses have more wiggle room than large ones -- they are not held to the same standards of accountability and records integrity that a large organization would be. However, remember that it is a judge who is going to decide this, which is why having a solid written policy is an important first step.

Your policy should be matched to your organization's document types and budget. Generally, I am in favor of automation and appliances if you can afford it. Building automated processes and buying an appliance or software package ensures your policy will live past any individual, and that you'll have some assurance that the procedures will pass muster in a courtroom because you followed normal commercial paths.

If you find that your organization just can't spend the time or money to build in automation, or if your systems are not amenable to an automated appliance, then fall back to something more manual (and error-prone). Another benefit of automated processes and systems is that, when properly done, they don't let IT cheat by rigging the system. If it's an IT issue at stake, your company credibility will be higher if you can show you made an effort to keep a privileged user in the IT group from being able to delete or falsify records.

When a small company is involved in a lawsuit, it's a pretty ugly time. Do your part ahead of time to ensure that IT is there to help.