

CIOs, Electronic Records and the Law

By Ed Sperling

19 July 2010

Forbes.com

How long corporations should keep documents and e-mail has always been a gray area.

In regulated industries there are clear-cut guidelines, but for most other companies these kinds of rules don't exist. The result is that most companies set their policies and forget about them until they get involved in a lawsuit. Then, suddenly, their retention policies and adherence to those policies get called into question--along with the CIO's job performance.

Just how nasty can all of this get? Forbes caught up with David Canfield, managing consultant for Kroll Ontrack's electronically stored information consulting group, to find out. Kroll Ontrack is the technology services unit of risk consulting company Kroll.

Forbes: What happens when e-mail or data gets lost?

Canfield: In the 1990s a corporation would say, "We have a few e-mails and a few documents" and they would agree to print them out for the legal teams. By 2003 the sheer volume of data made it impossible to review all of that in a traditional sense, and over the past 10 years a lot of the emphasis has been on the tools to search this data and review it in a much more efficient manner.

When Intel was sued by AMD it claimed to have lost e-mail. Is that a common problem?

Yes, and it's a very serious problem. Not all of these review platforms are created easily, and sometimes they lose e-mail or attachments. You often find the problem is the way corporations designed these systems. So there's been an explosion of archiving tools like Symantec's Enterprise Vault and Autonomy Zantaz. That's a typical knee-jerk reaction for corporations to use these kinds of tools--especially in the financial sector, where there are Sarbanes-Oxley requirements to keep e-mail and communications to the clients. Many of these systems have the option to remove attachments and store them separately from the e-mail. If you don't realize that you might find yourself in a position someday where you need to produce e-mail for litigation and it no longer has that attachment. That's exactly what happened in the Intel case.

What's the liability for the CIO?

From our past surveys we've seen that a lot of corporations blame any shortcomings in data directly on the CIO and IT. Thankfully a larger portion is blaming it on the CIO and the general counsel, but the CIO is still catching a lot of the blame. It is an immediate hit on their reputation and their position in the company. I have yet to see a CIO who is held legally liable, though, and there's a good reason for that. They chose a system that would put them in compliance with Sarbanes-Oxley, for example, and that choice was made because they thought they were doing the right thing. Without having a good understanding of the legal issues and the ramifications of the systems, a CIO may opt for the most efficient model. It's more efficient to have attachments stored separately and de-duplicated. Those decisions are based on the most cost-effective, time-effective and space-effective way to store data. They don't realize what the impact is down the road when it comes to litigation.

In many companies there has been high turnover in the CIO office. How does that affect these kinds of decisions?

Even though decisions were made before they took over that had negative ramifications, they don't typically survive those kinds of issues. It comes down to a basic understanding of what's required legally. One of the most common complaints we hear is that the IT and the legal groups within a company don't communicate with each other very well. They may use the same words or language, but each has entirely different meanings. And they don't take the time to come back and confirm what those meanings are.

Does it matter that many of the CIOs are coming out of a business background rather than technology?

It helps. But one of my favorite ways to win a lunch is to walk into a company and ask about their retention policy for e-mail. The response may be something like, "We're an Outlook shop, and we have 30 days retention on our e-mail." I'll challenge that and go find the e-mail administrator, who will typically tell me, "The inbox is 30 days, user-created folders are one year, the dumpster is 14 days and deleted items are seven days. And, by the way, our e-mail is on backup for 18 months." So their e-mail retention is 18 months or longer, and I've just won lunch. There's a disconnect even among the newer CIOs. A lot of these decisions were made by the corporate counsel or outside counsel who said, "You must keep this type of content for a certain number of years." But no one has gone back to the IT side and figured out what is happening inside. What's stated in policy and what the CIO believes is happening is not what is actually happening in their environment.

How much of this is past technology decisions being judged by current standards?

That certainly is an issue. It's not uncommon for a case that is three to six years old to be judged by today's standards. But that's the reality. Without very good documentation of why you chose certain policies, it's very hard to defend what you did when you first came into the CIO's office or what your predecessor did.

It sounds like a no-win situation for the current CIO.

Yes, and that's the unfortunate thing. What we recommend is that when you're making a policy decision, whether it's record retention or e-mail retention, don't be afraid to revisit those every six months. You need to be very mindful about what is really going on in your environment, and you need to be cautious or suspicious of recommendations that come down from the general counsel's office or from outside counsel. A lot of times these decisions are made in a vacuum, and they may be in conflict with what you're doing.

There are a number of things companies have been doing as a reaction to litigation that need to stop. You need to come back to how this will affect you two years from now. If you receive notice of an investigation and you have to keep all your data concerning a particular matter, your attorneys would send out a legal hold notice telling people with this type of data to preserve this data. They also should be sending a notice to IT saying that if there are any systems with a certain kind of data on it then it should be preserved. But IT doesn't think of content. It thinks of massive amounts of data. They don't know where content XYZ lives. The most common reaction is to hold all the backup tapes. So they've complied with the hold notice, but two years later when legal discovery begins the data they're looking for may only be on backup tapes. That means restoring tens of thousands of backup tapes to find the relevant data. It costs millions of dollars and the CIO didn't budget for this and had no way to know it was coming. The argument starts with legal about whose budget should pay for it and that typically starts the downfall of the CIO.

What should the CIO have done?

They should have gone through a data mapping exercise with people from each department or business unit to determine what content they actually create. So the next time one of these notices comes in, rather than preserving every backup tape for all 5,000 servers in the company, you only need to collect data from these three servers. It's more work up front and it requires a cooperative understanding between legal and IT, but the savings in cost, reputation and the risk of doing something wrong is greatly reduced.

How long should companies keep e-mail?

Unless a company is under some type of regulation that require it to keep the data around for a specific number years, like Sarbanes-Oxley or FERC [Federal Energy Regulatory Commission] regulations, a company can develop whatever policy it wants. It just has to stick to that policy. You have to create the policy, provide training on it and stick to it.

But when people really want to keep their e-mail, they'll find some way to have it for years. What we recommend companies do is separate out true business records and store that on a separate server.

Ed Sperling is the editor of several technology trade publications and has covered technology for more than 20 years. Contact him at esperlin@yahoo.com