

COMMENTARY

Reprinted From E-Discovery: A Thomson West Report

What Is Your E-Mail Retention Policy? No, Really, How Long Do You Keep E-Mails?

By Stephen Stewart and Johnnie M. Jackson Jr., Esq.

Such a simple question can be the source of tremendous debate and substantial hand-wringing when a simple response like “two years” is explored as part of a “meet and confer” during discovery in a lawsuit.

The last thing you want is to walk into a meet-and-confer with an answer to this question—*e.g.*, “two years”—only to have your credibility diminish and your confidence dissolve as your adversary methodically backs you and your IT representative into a corner.

While “two years” may be what the e-mail retention policy mandates, it is critical to have a complete understanding of why your organization, in all likelihood, will have e-mails that are much, much older.

And you’re not alone. Nearly all other organizations do find themselves in a similar situation.

So, *really*, how long do you keep e-mails?

The question, “What is your e-mail retention period,” will most certainly come up in any meet-and-confer, so it is a good idea to know:

- What your policy states.
- Who is responsible for setting your policy.
- Who is responsible for enforcing your policy.
- Exactly how it is enforced.
- Whose policy is it? The CEO’s, the audit committee’s, the IT department’s, the legal department’s?

Even if you know what your e-mail retention policy is, here are some ways to confirm it and, in the process, “test the system” to find out if anybody is actually adhering to what your policy mandates.

- Ask your CIO or someone from the e-mail management team.
- Check your organization’s e-mail retention policy document.

- Ask your departmental counterparts, call someone in finance and call someone in the business units.

In each case, you will likely get one of the following responses:

- We don't have one; the individual employee can determine how long to keep e-mail.
- We keep everything forever.
- We keep our e-mail for two years.

E-mail retention policies are only as effective as their implementation. One of the most costly mistakes an organization can make is to have a policy but not follow it. During the meet-and-confer, both sides are looking to present a well-thought-out discovery plan.

This includes relevant repositories, effective search strategies and what information is deemed accessible or "not reasonably accessible without undue burden of cost" under Federal Rule of Civil Procedure 26(b)(2)(B), as well as the effectiveness of the parties' processes and procedures. Presenting your e-mail retention policy in absolute terms, only to have IT say, "Well, actually, it's more like this..." is not something you want to happen. These types of inadvertent misrepresentations undermine the judge's confidence and can affect your credibility.

Common Answers to the Question: What Is Your E-Mail Retention Policy?

We don't have one.

Having an unlimited retention policy isn't necessarily a bad thing. Absent a statute, regulation, contract or business purpose, organizations can keep e-mails forever or delete them immediately. However, organizations still need to know what to do if litigation occurs. Regardless of the e-mail retention policy (none, forever, selective), organizations must be able to control e-mail retention once a legal hold is triggered. This includes identifying and preserving all potentially relevant e-mail, be it active, archived or "not reasonably accessible without undue burden or cost."

If you don't have an e-mail retention policy, you should strongly consider developing one. Many of the costs of e-discovery are associated with having to look in all possible locations for potentially relevant e-mail: mail servers, network shares, desktops, laptops, PDAs, iPods, etc. The risk of sanctions for not being able to identify relevant information and produce it is real.

Part of the high cost of discovery for businesses without an e-mail retention policy results from employees' use of personal archives. This can require searching in an ad hoc fashion without the benefit of planning and possibly with an incomplete understanding of where and how the organization stores its data. Controlling and internally regulating how employees manage their e-mails and other electronic data can save hundreds of thousands of dollars in e-discovery and review costs when a large organization is involved in litigation.

What do you know about how your employees use personal archives? A personal archive is a location where e-mail users can copy messages from the corporate mail server and store them for their personal use. Employees frequently resort to a personal archive when IT implements a mailbox quota that forces the employee to either delete e-mail or copy it from the corporate e-mail server to another location, typically their personal computer or network drive.

Regardless of the e-mail retention policy (none, forever, selective), organizations must be able to control e-mail retention once a legal hold is triggered.

Most corporations use either Microsoft Exchange (Outlook) or IBM Lotus Domino (Notes). Each of these e-mail clients allows users to create personal archives; in fact, they can prompt the user to automatically create them (PST in Outlook and NSF in Notes).

If you're not sure about your organization's use of personal archives, check with your IT department and ask how e-mail and personal archives are managed. If you wait to find out until the day of the meet-and-confer, it is most likely too late to really understand what your organization does and definitely too late to effect any meaningful change.

We keep everything forever.

Unfortunately, many organizations that are frequently involved in litigation fall into this category, including financial services providers, pharmaceutical companies and insurers.

If your organization keeps everything, you have a different set of challenges than do those with a limited retention policy. Your challenges revolve around managing and working with the archiving solution your organization has chosen to implement.

Symantec's Enterprise Vault, EmailXtender by EMC Software, and Zantaz's First Archive and other products have the most brand recognition, but numerous other archiving solutions on the market provide the same business values and benefits. A simple Web search for "e-mail archiving" will yield dozens of hits.

To start, learn as much as you can about the system your organization uses. These archiving solutions provide storage efficiencies and robust content indexing capabilities, but they are not perfect, and it would be wise for you to fully understand what they can and cannot do. Organizations with large archives should carefully monitor, maintain and test their chosen archiving solution to ensure it is delivering the expected results.

Here are some tips for effectively managing and searching an archive:

If you're not executing the queries yourself, stress the importance of this process. Make sure IT knows this is much more important to the future of the entire organization than the server upgrade that also needs to be performed.

Have someone in IT create a script that will send an e-mail every hour on the hour, 24 hours a day, 365 days a year with a piece of very unique but identifiable content. As a basic test, you can search for a given day, week, month or year and check the total number of hits. If you don't find all these messages, you can assume that queries made in response to a discovery or audit request will probably have gaps as well.

Take time to understand the nuances of your archive solution's query language. Just because you are familiar with Boolean search logic doesn't mean all vendors have implemented that logic in a consistent fashion.

Understand how the archiving system tracks and maintains e-mail addresses. Then build a business process to ensure the addresses are maintained. This information will be invaluable when searching foremployees who have been terminated or transferred, changed their names, or were integrated as part of a merger or acquisition.

Document your queries as well as the results. Nothing is worse than rerunning a query a month later and getting different results because you are using slightly different search terms.

If your organization keeps everything, you have a different set of challenges than those with a limited retention policy.

The corporate archive is not just another system—it is often the “system of record” used to produce evidence to the courts.

Build out a set of test data, including both positive and negative responses for each query. This can be used as a training tool for new investigators and a means of validating new product releases, and it will help build confidence in your process and the search tool.

Review the results. Don't assume they are accurate and complete. Look for things like breaks in date continuity. If Stephen Stewart gets 700 e-mails a week and then gets none for two weeks, you might have a gap. If keyword queries return 10,000 hits on average, but you just ran a query and the search engine returned 1,000, this could also indicate a gap.

Organizations should approach large e-mail archives with a great deal of rigor and discipline. Despite vendors' best efforts, their archiving tools still require a significant amount of care and attention to detail. The effective use of these solutions also requires a close interaction between legal and IT. It is important for everyone involved in the process to recognize the importance of the archive and the likelihood that its contents could be debated before the court. So take it seriously. The corporate archive is not just another system—it is often the “system of record” used to produce evidence to the courts.

Tips for managing and searching an archive

- If you are not executing the queries yourself, stress the importance of this process to IT.
- Have someone in IT create a script that will send an e-mail every hour on the hour with a piece of unique but identifiable content.
- Take time to understand the nuances of your archive solution's query language.
- Understand how the archiving system tracks and maintains e-mail addresses.
- Document your queries so that you use the same search terms each time.
- Build out a set of test data, including both positive and negative responses for each query, to help build confidence in your process and the search tool.
- Review the results. Don't assume they are accurate and complete. Look for breaks in date continuity.

We keep our e-mail for two years.

In an effort to control the overall amount of e-mail that must be managed, IT is adopting strategies that force employees to make basic decisions about which e-mail to keep.

In Microsoft Exchange (Outlook), for example, employees can keep e-mail in their Inbox for 30 days and in their personal folders for two years.

In an ideal world, employees would keep only relevant business records, but this is often not the case. An automatic deletion policy forces an employee to file a message that is important enough to keep in a personal folder. Otherwise, it will be automatically deleted after 30 days. Once filed into a personal folder, the e-mail can sit there for up to two years before being deleted. If the e-mail has no value, the employee can simply let it sit in the mailbox, and the automatic disposition process will delete it after 30 days.

It is important to understand what is actually meant by a “personal folder.” In Outlook, “personal folder” can mean a folder created by the employee on the Exchange server or a personal archive, known as a PST, that the employee has

created to archive e-mail outside the Exchange server. If your organization allows PST files, you need to go back and read the first part of this article because you really don't have an e-mail retention policy.

Consider what happens to the e-mail once it is two years old. Does it disappear completely or does it still linger?

The Microsoft Exchange server allows an Exchange administrator to configure the number of days a message can exist in a certain folder before it is moved to another folder. In most instances, messages move from the employee's Inbox into the Deleted Items folder, where they can stay for several more days or weeks. So immediately, the two-year retention is actually two years plus the amount of time that an item can sit in the Deleted Items folder.

It is also possible the item still isn't truly deleted from Exchange after leaving the Deleted Items folder because it can still exist in the Exchange Dumpster. The Exchange Dumpster can be configured to catch all deleted items, included those that the employee "permanently deletes" and those emptied from the Deleted Items folder.

In a very basic configuration, a two-year retention can be more like two years and two months. Make sure you understand the specifics of your configuration before you make incorrect statements to the court.

In Lotus Domino (Notes), employees can keep e-mail in their mailboxes for up to two years.

Domino does not natively offer the same degree of control for managing individual folders as Microsoft Exchange, but what an organization loses in flexibility, it gains in risk reduction. If your organization uses Lotus Notes you should follow up with the Notes administration team with the following questions:

- Do we use Lotus' native archive policy or something else? If you use the native policy settings and they are configured to delete all documents older than two years, Lotus will automatically delete items. It will not remove the e-mail in stages but rather immediately remove them from the mail file.
- Do we allow "soft deletes," or does a message immediately get removed from a user's mailbox when the trash is emptied? A soft delete is a setting that can be used to automatically delete e-mails from the trash folder after a period of time defined by the user. This staged deletion gives you a chance to retrieve messages if you make a mistake.

These examples do not include the time associated with backup retention or the existence of a corporate archive. If you have a corporate archive or your organization allows personal archives, you are more likely to consider the above advice. However, if you do have a corporate archive, the information stored on the e-mail server cannot be older than what is stored in the archive; if so, you have totally defeated the purpose of an archive as your system of record.

What Does It All Mean?

Despite all the nuance of how organizations implement an e-mail retention policy, one thing is for sure: An organization must have the ability to override that policy when litigation is reasonably anticipated. However, in many organizations, the appropriate communication protocol and exception-handling process are not in place to manage an effective legal hold. Failure to stop the automatic disposition of e-mail has led to a variety of sanctions as well as forced organizations to produce data from more costly sources:

Failure to stop the automatic disposition of e-mail has led to a variety of sanctions as well as forced organizations to produce data from more costly sources.

eDiscovery: A Thomson West Report

- \$2.75 million monetary sanction: *United States v. Philip Morris USA Inc.*, 327 F. Supp. 2d 21 (D.D.C. 2004).
- Order to produce e-mail from backup tapes: *Disability Rights Council of Greater Wash. v. Wash. Metro. Area Transit Auth.*, 2007 WL 1585452 (D.D.C. June 1, 2007).
- Adverse inference instruction: *DaimlerChrysler Motors v. Bill Davis Racing Inc.*, No. 03-CV-72266 (E.D. Mich. 2005).
- Adverse inference instruction and \$10,000 monetary sanction: *ETrade Sec. v. Deutsche Bank*, 230 F.R.D. 582 (D. Minn. 2005).

Organizations that hope to claim protections under the safe harbor afforded by Federal Rule of Civil Procedure Rule 37(f) are going to have a hard time claiming that the data was “lost as a result of the routine, good-faith operations of an electronic information system” when repeated case law and simple legal-hold notices are frequently requiring that the automatic disposition be disabled. In light of these expectations, the legal team needs to work with IT to understand how and exactly what is done when the hold notice is issued.

Be prepared! You should take the necessary time now to understand what your policy says and how it is actually implemented *before* you are asked to describe it to the judge.

Stephen L. Stewart is an expert in archiving, discovery and data management strategies for risk reduction. He has worked for OTG Software, Legato and EMC where he held a variety of technical roles including consultant, systems engineer and product manager. He is a principal with ESI Strategies and can be reached at [sstewart@esistrategies.net](mailto:ss Stewart@esistrategies.net) or (800) 842-4252.

Johnnie M. Jackson Jr. is an attorney, board member, governance consultant and former vice president, general counsel and secretary of Olin Corp. He is lead director of ESI Strategies' advisory board and can be reached at jjackson@esistrategies.net or (800) 842-4252.