Records Retention for Industrial Manufacturers

Check the cazh1 web site (www.cazh1.com) for updates to this document.
The **Last Update**: date in the lower right corner is your indication of freshness.

Executive Summary

> *[Records Retention refers to] the practice of maintaining records for an organization from the time they are created to the time of their disposal. (source: Wikipedia)*

That last bit is the tricky part; every day at most corporations eMails, spreadsheets, and presentations (collectively: “stuff”) are created, shared, and printed – along with all of the financial and transactional records issuing from the various ERP / accounting systems. Creating stuff is easy – but are we rigorous enough in the “end of life” phase, when documents that *should be* destroyed *are in fact* destroyed?

There is potential risk in the growing pile of stuff – which is why companies implement Records Retention policies that specify what documents are to be retained, for how long – and mandate which documents must be destroyed after a certain period.

Implementing a comprehensive Records Retention policy is not an easy task – these projects often generate significant organizational change issues (as well as a lot of expense). Over the past few months, I have found myself drawn into these conversations with a number of IT professionals in my personal network; as a result, I thought it might be interesting to conduct some loosely structured “market research” to collect some thoughts on the issue.

> **NB**: This version of the document [subtitled *Bootstrap Market Research*] has had identifying information removed from the source data, and has been circulated with the surveyed companies and posted on my www.cazh1.com.
>
> If you care to add some information, I'll thank you in advance, and add it (sufficiently anonymized) to this summary results document; the **Last Update:** date in upper right corner of each page is your indication of freshness (compare to the date of the file on the web page).

Important Definitions

eMail Retention policies limit the amount of mail that can be stored in your corporate eMail account. Often referred to as “limiting the size on your Inbox [or Mailbox]”, these policies are in place to minimize the storage space and backup requirements (and the associated costs).

Records Retention policies specify the amount of time that different records must be retained, and mandate the *complete destruction* of these records after that time. These policies are in place to minimize exposure to lawsuits based on ill-conceived or damaging documents, and minimizing exposure to large *electronic discovery* costs.

> **NB**: For electronic records such as eMail, “complete destruction” means deleting the file(s) *plus any and all backups*.

Electronic Discovery (aka eDiscovery) refers to the process of identifying and analyzing electronic records that are potentially relevant to a legal proceeding. If an organization does not have a comprehensive and consistently implemented Records Retention policy, eDiscovery can be a very expensive and time-consuming process.

PST refers to an external message storage format for Microsoft eMail users. To reduce the size of your mailbox, you can save message to a PST file on your hard disk. This *helps* an eMail Retention policy because it reduces storage requirements on the mail servers; it *hinders* a Records Retention policy because these files are very expensive to include in an eDiscovery project (but you will have to do it!).

> **NB**: Some of the respondents in this survey are Lotus Notes eMail users, which has a similar capability under a different name. Since Microsoft users are in the majority, we are sticking with that terminology throughout the document.

Methodology

We have chosen to focus on retention policies and procedures for eMail, which is …

- … a subset of the overall set of records in a comprehensive Records Retention policy
- … the primary source for organizational angst and implementation cost (ie. the hardest behaviors to change)
- … the largest element of potential risk to the portion of the most and implementation cost

Phone and/or eMail interviews were conducted with the IT infrastructure teams responsible for implementing these policies at the selected companies.

Questions

1. Do you have an eMail Retention Policy? What does it cover – email storage space (inbox size)? Time limits / automatic deletion?

Some specifics … if they apply …

   a. What is the max space allowed for an email account?
   b. Any exceptions (by role / department, for certain individuals, other)?
   c. How many months can an email remain before it is automatically deleted?
   d. Do you allow users to save eMail externally (for example, in MS Exchange – do you allow PSTs?)
   e. What do you do with eMail and eMail accounts of exiting / former employees?

2. Is this an actual corporate policy (subject to audit, reviewed and signed off by each employee, backed up by proof of compliance) or just a standard set up / configuration for the eMail environment?
3. When was your policy implemented – and why? What was the primary justification (save space, reduce eDiscovery costs, reduce eDiscovery risks, other)?
   a. Who originally sponsored the program / standards / policy?
4. Who is responsible for ongoing training & re-affirmation of the policy / standards?
   a. Is training available?
   b. Is it scheduled (with a trainer) or "on demand" (self-service, web based)?
   c. Is it part of any New Employee onboarding process?
   d. Is it part of any recurring training and certification / signoff / acceptance for existing employees?
5. Backup and restore
   a. Is all eMail backed up? Part of the Disaster Recovery planning?
   b. Do you keep historical backup tapes? If so, how far back?
   c. Do you have any expectations/ SLA / SLO for ability to restore eMails?
6. Any questions you would like to hear about from other, similar companies?
7. May we share your answers anonymously (ie. without identifying your company)?

Results

Summarized Findings

Company	Industry	Revenue	Records Retention ?	eMail Retention ?	eMail Storage Limits	PSTs Allowed?
"StrictCo" highest level of document control			●	●	Yes	No
KLKL Co.	Manufacturing (machinery)	$$B	◕	◕	Yes	No
HIHI Inc.	Manufacturing (industrial)	$$B	◑	◑	No	Yes
CDCD Co.	Manufacturing (machinery)	$$B	◔	◕	Yes	Yes
FGFG Corp.	Manufacturing (energy)	$B	◔	◕	Yes	Yes
DEDE Ltd.	Manufacturing (industrial)	$$B	◔	◑	Yes	Yes
BCBC Inc.	Manufacturing (electronics)	$B	◔	◑	Yes	Yes
MNMN Ltd	Manufacturing (industrial)	$B	◔	◑	Yes	Yes
ABAB Co.	Pharmaceuticals	$$$M	◕		No	Yes
LMLM Inc.	Manufacturing (electronics)	$$$M	◑	◑	Yes	Yes
JKJK LLC	Manufacturing (infrastructure)	$B	◔	◔	No	Yes
"LooseCo" lowest level of document control					No	Yes

The circular quadrants ( ) indicate degree of strictness & completeness for the *Records Retention Policy* and *eMail Retention Policy* columns, with the two end points (the fictional "StrictCo" and "LooseCo") representing the extremes:

		StrictCo	LooseCo
Records Retention Policy	●	• Written policy • Requires document destruction • Support for Records Hold • Measureable and enforceable (allowing limits on eDiscovery requirements)	• Unwritten or non-existent policy • Suggest document destruction or completely ignores the issue • Lack of standards renders it un-enforceable – no limits on eDiscovery requirements
eMail Retention Policy	●	• Written policy • Recurring education • Reasonable limits on eMail storage • Support for Records Hold	• Unwritten or non-existent policy • Limited education • No limits on eMail storage size • Backups kept indefinitely

ABAB Co.

$$$M manufacturer of pharmaceuticals

eMail exchange with Vice President, Information Technology

No eMail retention policy exists / none is enforced – but they do capture a copy of all inbound and outbound emails in an email archiving system. This was done so legal could guarantee they could demonstrate that emails in question are the only emails ever received / sent on a topic; it guarantees that no emails are ever lost.

PSTs are allowed, but it is perceived that few use them – since all eMail is archived.

All eMail is outsourced, an arrangement that includes archiving all mail.

When employees leave the company, their accounts are summarily deleted; a purely mechanical process, as all mail is getting archived.

Live eMail accounts are backed up every night, and the outsource provider keeps 3-4 days of backup tapes. Beyond that – they rely on the archiving solution.

BCBC Inc.

$B manufacturer of electronics

eMail exchange with Chief Information Officer

eMail retention policy is loose, but does exist; there is an education / information process when someone starts with the company, focused on proper use and acknowledgment that this is company property. There is an annual signoff for all employees.

Mailbox size is not strictly limited, default set to 1G and some key roles within the company get more.

There is no automatic deletion of eMails, but note that they only keep 6 days backup in tapes. Anything removed from the Deleted folder is irretrievable after 6 days. There is no express or implied Service Level Agreement (SLA) / guarantee for eMail restores.

PSTs are allowed.

When employees leave the company, access to their accounts is delegated to another person in the department. Incoming eMails are allowed for a period of time, so as not to miss any important communications.

CDCD Co.

$$B manufacturer of machinery

Phone call with Consultant from Some Vendor, who was with CDCD when they went through their Records Retention / eMail Retention project

- CDCD was already archiving and deleting emails after a certain amount of time; trigger issue was an event that required discovery against that email. It was very difficult for Legal, and they were looking for something better
- However, they are still not destroying anything per se – the focus was solely on what was located in the MS Exchange email system
    - They still cannot reliably access to archives/ backups
    - Legal team could do some review, but was not smooth
    - No way to guaranty disposal of “smoking guns” – an acknowledged risk
- Has initiated a project to look at this larger risk, to solve those three issues, but [source] does not have a recent (within 6 months) update on status.
    - Source assumes little is happening because the effort slowed to a halt when they were still involved

Two other notes from source (in the role of Industry Professional)

Pharmaceutical and Financial companies focus on “risk” (around litigation from smoking guns and potential eDiscovery costs), while Industrial Manufacturing focuses on “cost” (in terms of required storage and backup costs from expanding eMail inboxes).

DEDE Ltd.

$$B manufacturer serving industrial markets

Phone conversations with Global Information Security Director

- A recent merger here - the “legacy” business had an eMail Retention policy, the DEDE “parent” did not. The newly merged organization is working to implement a comprehensive eMail Retention policy but it is tough.
- In the past (with LegacyCo) and now – there is no policy on Records Retention, or a rigorous policy to destroy stuff.
- They do have an eMail retention policy, focused on eMail inbox size
    - A valid way to address this problem – move your email to your hard disk (PST). So – you can’t ensure the mail is deleted, so you still have to eDiscover it.
- eMail Retention policy / program started when they converted from an older Notes eMail environment to MS Exchange (cost and complexity identified the storage cost challenges)
- Currently, their eMail inboxes are limited to 25GB, and they don’t have any retention policy as long as it fits.
- The current strategy for eDiscovery – they have kept all backup tapes from older eMail systems. However, there is no guarantee that they will be able to restore from them.
- They have been sued and been compelled to do eDiscovery; most notably related to the [*something interesting I just have to edit out, sorry – jpm*].
    - They have had to put some 25M pieces of eMail on hold – but apparently it has not been expensive enough yet to implement fill Records Retention
    - When there are eDiscovery expenses, the Legal Department covers the cost.
    - Since the backup tapes of old eMails are done solely for the purpose of potential legal eDiscovery, the Legal Department pays for the tapes and the storage.
- There is no formal training available for the process of cleaning out / making backups of the employee’s eMail – but the process is considered straightforward, and most are comfortable with the steps.

FGFG Corp.

$B manufacturer for the energy industry

eMail exchange with Director of Information Technology

There is an eMail retention policy in place, documented in their financial standards.

The policy is focused on size of the mailboxes. All employees are allowed 400Mb, and certain key employees can have their mailbox expanded to 1GB; there are no mailboxes larger than 1GB.

eMail is automatically deleted after 45 days; however, PSTs are allowed for offline storage of eMails

eMail accounts for departing employees are kept for 30 days, then archived and removed from the system

Training on the policy is part of the employee on-boarding process

Updates to the policy are reviewed annually, based on changes or updates in the supporting technology

The eMail system is part of their Disaster Recovery process

eMail is regularly backed up, and tapes are kept for 30 days before being written over with new data. No backups are available beyond 30 days.

HIHI Inc.

$$B industrial manufacturer

eMail exchange with Director of Corporate Infrastructure.

Their current eMail retention policy covers deletion of eMails, not mailbox size. In fact, there are no restrictions on mailbox size.

Automatic deletion is in place for items in the sent and deleted items. Sent items are purged after 60 days and deleted items after 30 (corporate policy).

For items not in the Sent or Deleted folders: Employees are instructed to save only those electronic communications that are considered “business records” (defined in corporate policy) and only for as long as they are useful, all others should be discarded.

1. There is no automatic deletion of received messages; if a message is not identified as marked Sent or Deleted, it could exist for the tenure of the employee
2. This is not a universal rule: exceptions are granted for individuals whose communications are on litigation hold (potential or pending litigation), international employees (due to specific country requirements), key executives, and the entire legal team

Employees are allowed to save their eMail outside of the eMail system, using PSTs.

When an employee leaves the company …

3. If a former employee’s communications are not on litigation hold, the employee manager has 90 days to review their email and save/copy relevant information to their or other team members mailboxes (standard process, unenforced).
4. If the former employee is on litigation hold, the account information will be retained for as long as the litigation hold is active (corporate policy). Once the litigation hold is released, the data is retained for 30 days and then purged (standard process, unenforced).

Corporate Policy that governs these issues was enacted in 20xx by the Legal department and General Counsel. At that time the policy did not have the automatic deletion clause. The primary goal was to reduce eDiscovery risk and costs.

5. In 20xy the policy was updated to include the automatic deletion of sent and deleted items. The justification was two-fold; save space and continue to reduce cost and risk associated with eDiscovery.
6. Training is available on both the Record Retention and eMail Retention policies. Training is available online only. Each employee has required annual training. A handout on the high level requirements is included in new employee orientation along with the requirement for the annual online training.

eMail is backed up on a limited basis. eMail backups are retained for no longer than 1 month, except for the tapes containing data on litigation hold which is retained as long as needed.

JKJK LLC

$B manufacturer of infrastructure stuff

eMail exchange with CIO

There is no specific eMail retention policy or guideline in place, aside from an Appropriate Use policy that is signed when an employee starts with the company

There are no size limits at this time on eMail storage; they have specialized software that enables incremental storage to be added. No automatic deletion of eMails

PSTs are currently allowed, but since there are no storage limits, this policy will be reviewed when they upgrade their eMail system.

eMail accounts are kept for departing employees for 90 days, then burned to CD for an additional 30 days. If no request is made to retain the information, it is deleted and backups are destroyed.

The eMail system is backed up by their service provider (eMail hosting is outcsourced); backups are available for 21 days.

KLKL Co.

Private manufacturer of machinery

eMail exchange with Director, Enterprise IT Services, and Director, IT Operations

Planning the implementation details of a revamped set of eMail policies:

eMail retention rules covering size of user mailboxes; limited to 1.5GB.

eMail retention rules covering age of eMails; all eMails will get deleted after 13 months; no archiving (PSTs) is allowed.

There is no backup of the eMail system

This is all part of a larger Records Retention policy that was driven by the Legal group and co-sponsored by the IT group. The intent is to change working habits, so people stop filing things using eMail and push them to SharePoint where they can be treated like a corporate asset, and more easily shared internally and externally, when appropriate.

There will be provisions for Legal Hold, and differentiated Records Types, so different policies can be enforced for different types.

Legal group has responsibility for ongoing training and re-affirmation of the policy; however, no training process currently exists, a work-in-process.

It is part of the employee on-boarding process, and there is a yearly reminder / reaffirmation sent out.

LMLM Inc.

$$$M manufacturer serving electronics industries

eMail exchange with CIO

Currently have an eMail retention “policy” covering size – but the size limits are very restrictive (250-500MB), and exceptions are the rule.

No automatic deletion is in place for eMail of current employees. On the other hand, there is no policy / process of retaining emails / accounts for former employees; they are just deleted.

The “policy” is actually more like an operational standard and technical configuration standard – there is no formal education or audit process in place.

IT and HR share ownership of the operational standards and training.

Training only occurs when a new employee is on-boarded, en masse for any M&A activity, and also if/when the policy is updated.

eMail is considered a critical system; it is regularly backed up, and they have replication [real-time backup] in place. Historical backup tapes are kept in perpetuity.

They have a stated expectation for restore time (for lost eMail) of less than 2 hours.

MNMN Ltd.

$B manufacturer of industrial equipment

eMail exchange and discussion with CIO

They have an eMail retention “policy” covering size and retention, but the limits are somewhat loose (3GB max mailbox size with exceptions for key employees, 5 years retention in an archiving system).

No automatic deletion is in place; eMail that is supposed to be retained is moved to an archive, where it is kept for 5 years.

PSTs are typically not used - the online archive is where the backup / large / old files can be kept. PSTs are used when an employee leaves the company – their account is backed off to PST and then deleted.

This is primarily governed by a standard set up and operational process; there is no actual company policy covering this. This program (online archive) was started over a year ago by then then-CIO as part of an overall move-to-the-cloud strategy.

Training occurs when a new employee joins the company; no scheduled re-training or re-affirmation occurs.

Other

Some questions coming back from the companies, looking for more information …

> What tools are organizations implementing, and do they focus on eMail only or support broader records retention? [IT folks like to think in “concrete” things, like software tools]
>
> How much time / cost is actually being spent on eDiscovery work to date? How real is this concern? [It’s very infrequent for some respondents, and they are looking for broader insight]
>
> How does private cloud vs. public cloud get impacted by Records Retention needs?

Contact Information

Questions? Comments? Suggestions? Let me know …

James P. MacLennan
jpmacl@cazh1.com
www.cazh1.com