contoural

White Paper

How Long Should Email Be Saved?

Sponsored by Symantec, Inc.

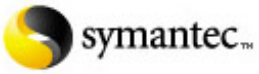

Table of Contents

***Note**: Legal information is not legal advice. Contoural provides information pertaining to business, compliance, and litigation trends and issues for educational and planning purposes. Contoural and its consultants do not provide legal advice. Readers should consult with competent legal counsel.*

Introduction

As email has become more critical in the business world, many companies are weighing the question of how long it should be retained, what should be done with it, and when it should be deleted. The answer depends on many issues, particularly when one considers the varying regulations and business situations that might demand emails to be archived for long periods of time. This white paper examines the reality of records retention and email archiving, focusing on the process of developing an effective retention policy and automating solutions to enforce rules and satisfy retention obligations. Contoural will also recommend best practices for email retention and real world examples.

Considering Email retention

As many high-profile cases have shown, failure to comply with an e-discovery request for e-mail as part of the litigation process can have a tremendous impact on businesses. Numerous internal policies and external regulations call for long-term retention and preservation of email, and many business circumstances demand recovery of historic messages as well. To ensure organizations will be able to meet these twin demands of litigation and legislation, all organizations, from the smallest private companies to the largest government agencies, must create a policy regarding long-term storage and handling of email messages.

Recent studies show that nearly half of all companies have some policy for email retention, but less than one in eight has implemented an automated solution to ensure requirements are met. Having an un-enforced policy is the worst possible scenario. Organizations can be held legally liable if their policies are not strictly followed, and only an automated system can help ensure compliance.

Email is a special, and critical, example of an application that, by default, lacks retention enforcement. Modern email systems are designed to be the hub of high-volume, daily communication. Applying record retention periods usually requires the addition of a third-party application. Relying on users to manually apply corporate retention policies is not only naïve but technically impractical.

Manual vs. Automatic

When considering e-mail message retention, IT organizations have a key decision to make:

Should users manually classify messages?

or

Should an attempt to be made to automate this task?

Manual classification is simpler to implement, but difficult to get right. As users decide which messages to keep and how to classify them, inconsistencies are bound to spring up, and productivity is lost. Automation can ensure consistent classification, but it is difficult to create a system that recognizes the nuances of business communication. An ideal system would combine the best of both worlds, automating simple tasks and requesting user input for more complex decisions.

The daily volume of email entering and exiting each user's mailbox, multiplied across the entire enterprise, necessitates an automated solution to enforce policy.

Email has other unique aspects as well. Although email has more structured metadata than most corporate applications in the form of headers, some content lacks standards. Subject lines, or even addresses, cannot be relied upon to be specific, consistent, or unique. The proliferation of email attachments creates another unique challenge, with encoded files frequently retransmitted and often containing key contextual information. Ironically, the flexibility of email as a communication mechanism undermines its inherent structure.

Over the last few years, email has also become the primary target for discovery requests during business related litigation. Here again, the flexibility and democratic nature of e-mail communication works against the needs of corporate counsel. In the event of a legal hold request, all relevant files and emails must be immediately preserved, and most e-mail software is incapable of this type of retention. Litigation hold is a joint responsibility of both the IT staff and the legal department, so it clear process must be put in place to communicate hold requirements. This communication must include information about the date and scope of the request, which locations and employees are covered, and the specific records or content that must be retained. Since legal actions can sometimes drag on, IT must also consider how it would handle continued retention for a long period of time.

Can IT Set Email Retention Policy?

Although IT organizations have proven adept at creating and managing complex technical systems, the creation of business policies has often proven troublesome. Indeed, it is unrealistic to expect the technical organization to create business policy in isolation. Instead, a consensus must be developed with a wide range of opinions throughout the organization.

Although the final, complete policy for email retention cannot be produced by the IT staff alone, they can produce a workable draft policy grounded in the technical capabilities of e-mail archiving software. Once this draft is circulated, it can be tuned to meet the expectations of the business, and integrated into a wider record retention policy. In general, the input from legal, finance, human resources, and business units will be integrated with the consensus from IT management, storage, and messaging representatives.

Best Practices

Although policies vary based on business circumstances, some universal best practices can be distilled from the experience of many organizations. The following practices are applicable to most email retention systems:

1. An email archiving policy should be part of an overall records management program, which has its own record retention policies and procedures.
2. The scope of the policy should consider all employees who create, send or receive email messages and attachments.
3. The email archiving policy should refer to IT's Acceptable Use Policy and expand upon the areas specifically related to email use.
4. The policy should state whether users can create PST files to store email messages.
5. Data privacy issues should be addressed. Employees should have no expectation of privacy when using company resources for email and could be subject to discovery proceedings and legal actions.

6. The policy must clearly state how and where email records will be managed, protected and retained.
7. The policy should explain how IT handles exceptions to the retention settings (e.g., some countries will require significantly longer retention periods for certain types of records).
8. Managers and users must be provided with training and support.
9. Compliance with the policy must be mandatory for all employees and include compliance in an internal audit review.
10. Review the policy yearly to ensure compliance with any changes or new regulations.

Taking these best practices taken into account and adding any organization-specific element, a draft email archiving policy can be created by IT as a way to kick-off an overall record retention policy modernization effort.

What Does An Email Retention Policy Look Like?

The key to creating an effective automated e-mail retention system is to keep the retention policy as simple as possible. Not only does simple approach assist in implementation, it also allows ongoing management and monitoring using common sense rather than complex rules. Therefore, an effective email retention policy should be short, specific, and cover 95% of all message traffic. Any exceptions will be handled manually as needed.

One key question to answer when creating an email retention policy is the length of time that most messages will be retained. In addition to the cost of long term storage, there are risks in retaining data as well as in deleting it. Most companies come to the conclusion that many messages should be retained for a few years for business productivity purposes. Once retention stretches beyond the memory of users, it must be indexed and searchable, which normally means keeping messages online rather than on tape.

Determining Email Retention Periods: Keep it Simple

Over time, the cost of disk storage continues to decline while the length of time messages are retained climbs. Could email storage costs become irrelevant? For instance, the total size of a large enterprise messaging system from ten years ago was likely to be measured in megabytes while five years of email storage may be measured in the tens of gigabytes. Although these appeared to be large numbers at the time, they are small compared to today's enterprise storage capacity. Assuming the cost per gigabyte of storage continues to decline, one could deduce that all messages should be retained forever,.

Elements an Email Policy

An email-retention policy should cover all employees, contractors, and others related to the company who create, send, or receive e-mail messages. It should be clear that, in addition to the message body, attachments and headers, including addresses and hidden information, are also part of the policy.

The email policy must specify the following standards:

- Acceptable use of the email system
- Unacceptable uses of email
- Offline copies of email messages
- Privacy issues and local regulations
- Email management and retention policies
- Responsibilities of the staff
- Auditing and processes for dealing with violations

However, there are risks with long-term retention. As the volume of messages increases, the cost of complying with e-discovery request increases as well. A higher volume of messages combined with more powerful search capabilities, can lead to escalating demands on the IT and the archiving solution. A larger message store could also expose the company to legal entanglements, (i.e., the "smoking gun" email message), that otherwise could have been avoided if messages were routinely deleted. In the end, the risk and cost of long-term retention must be balanced against the desire for a complete archive of email messages.

General Business Correspondence

As stated earlier, the goal of an email archiving solution is to automate the retention, expiry and classification and retention of 95% of all messages. When creating an email retention policy using an automated solution, group messages with similar retention needs logically such as by function, department or title. Most email messages can be classified as general business correspondence with a suggested default retention period of three- to five- years. This single rule will probably cover the majority of all email messages.

Functional Departments, Titles or Names

Next, find universal and logical criteria to identify and classify the remaining email messages. Experience has shown that two more key criteria will cover these communications: critical organizational departments, and key individuals. Critical departments typically include finance, which may need a retention period of ten years or longer for tax purposes, as well as human resources and legal staff. Certain key management figures or company officials may need indefinite retention of email messages. Include corporate executives, who may have a fiduciary responsibility to the company, as well as directors and members of corporate governance boards.

Managing Exceptions

A small percentage of email messages will have to be categorized manually. Employees will need to be trained on how to recognize which messages will be exceptions to the general policy, as well as what their retention period should be. Of particular importance are apparently mundane messages whose attachments or context make them critically important. These will have to be managed manually by those familiar with their content. The retention period for exceptional messages will require some research into the specifics of an organization's business functions, and must be done with an eye toward a larger record retention management program.

Regulatory Compliance Requirements

A wide variety of regulations and standards apply to record retention, and email can be a vehicle for these records. Different regulations will apply to different departments within every business – human resources may concern themselves with HIPAA, facilities may be concerned with OSHA, and finance may focus on Sarbanes-Oxley. Therefore, it makes sense to target the email archiving solution by department or area of responsibility in order to align it with record retention regulations.

The table below shows many of the regulations that might affect record retention and security requirements. Some affect certain market sectors or corporate constituencies, while others are region-specific or focus on public companies or manufacturers.

Sector-Specific Regulations	Financial Services			Health Services		Life Science	
	SEC Rule17a-4	PATRIOT Act	Basel II	HIPAA	CMIA	21 CFR 11	UK GMP
USA Regulations	Sarbanes-Oxley Act (Enforced by SEC)						
	EEOC						
	OSHA						
	Gramm-Leach-Bliley Act (GLBA)		SB 1386				
UK Regulations	Data Protection Act (UK) and similar laws implementing EU Directives			EU GMP Directive 91/356/EEC-9			
	UK Public Records						

Note that most regulations do not specify the mechanism or schedule of record retention. Instead, they detail the desired outcome, whether that is protecting confidential information or producing critical records on demand. However, some regulations do specify retention periods for certain record types, as illustrated below.

Regulation	Focus	Area	Years of Retention	Note
21 CFR Part 11	Life Sciences	Clinical trials	35	Thirty five years from creation
		Food manufacturing, processing, and packaging	2	Two years after commercial release
		Drug manufacturing, processing, and packaging	3	Three years after commercial release
		Manufacturing of biological products	+5	Five years after the end of manufacturing
HIPAA	Healthcare	Pediatric medical records	<21	Until age 21
		Adult medical records	<+2	Up to two years after a patient's death
		Documentation related to security	6	Six years from date of creation
Sarbanes-Oxley	Public companies	Audit-related records	+7	Seven years after the conclusion of the review
SEC 17a-4	Financial services	Account records	+6	Six years after closing the account
		Financial statements, transaction records, communications	3	Two years easily accessible, three years total
		Member registration and corporate documentation	∞	For the life of the enterprise

Note retentions vary relative to different areas of focus: Some concern the lifespan of individual people, others refer to the beginning or end of a product's development, and others are specific to a document or other record. When they take effect also varies – some start counting at creation while others are "term plus", adding years after an event. Another

consideration is whether the regulation calls for a positive end or not – some demand an action at a certain time, while others are minimums.

This can get quite confusing. HIPAA, for example, calls for retaining adult medical records only for two years after a patient's death but retaining pediatric records until the patient reaches the age of 21. This means that a retention scheduler would have to have access to birth dates and death records, which would likely be injected come from an outside source. Automating this type of retention schedule can test the flexibility of both the archiving product and the programmer assigned to implement it.

What Are The Key Elements Of An Effective Records Retention Program?

Automating email retention should be a key element of an enterprise-wide records management program. Other elements include: the creation of a core team to direct each project, assessment of business and technology requirements, implementation of an email-archiving system, education and training, and monitoring and auditing.

Create a Core Team

The creation of a records retention policy will be the foundation of a bridge between IT and the legal staff in an organization. In many cases, these individuals will have rarely interacted with each other, but records retention is one shared area of responsibility, and email-archiving is often the first step. Therefore, the first key element of an effective records retention program is a meeting of minds between IT and the legal staff. Additionally, human resources, finance, business functions, and other non-IT individuals are likely to be interested in records retention.

Assessment

The first action of this joint team will be an assessment of the business and technical needs for record retention. An overall record types inventory must be created for all of the record types found within the organization. Consensus must be developed on the overall e-mail retention policy and gaps between this policy and the reality of email retention must be uncovered. Additionally, the organization's litigation-hold process should be investigated.

The process for dealing with litigation-hold requests and e-discovery should be codified and documented as well. In many cases, IT and legal staff may have previously struggled through e-discovery requests and these lessons can be brought to bear when creating the new methodology. Otherwise, the creativity of the legal and IT staff will be needed to ensure that a reasonable procedure can be put in place to deal with these critical requests on the archiving system.

Record Retention Policy and Schedule

In some cases, an existing record retention policy may already be in place. The policy should be updated to reflect any new regulations and refreshed to reflect the technical capabilities of the email-archiving system. If a record retention policy and schedule does not exist, now is the time to create one.

A simple record retention schedule can follow the simple logic of the number sequence, 1, 5, 10, 50 and 100. The minimum retention would be 1 year, with most general business correspondence retained for 5 or 10 years. Certain legal, financial, and contract items will require between 5 and 10 years of retention, so they can be placed at 10 years to be on the safe side. Exceptions

requiring longer retention can be placed in a 50 year bucket, which will likely outlast the archive system itself, or could be set with no expiration date. By using a simple retention schedule with just a few time periods, users will more easily understand the implications of their retention choices and overall system management will be simplified.

Retention Schedule Example

A retention schedule specifies the amount of time that a given record type will be retained. The example below illustrates a simple policy implementation schedule for different types of e-mail. Although these guidelines may be appropriate for some organizations, each will have to examine their own record retention needs to develop an appropriate schedule.

Default for most emails		5 years
Retention by Department or subject	Product Marketing	5 years
	Legal	10 years
	Human Resources	10 years
	Finance	10 years
	Executive Staff	50 years
	Engineering Development	50 years
	Regulatory Compliance	50 years
Exceptions		Determined by user

Solution Implementation Planning

If an archiving application is not already in place, the team must develop an overall strategy and implementation plan for such a system. This plan might include vendor and product selections, an RFP, and installation of e-mail archiving software. Although the core team may not be involved at every stage of this implementation, their oversight and energy will be needed to make it a success. Implementation of an email-archiving solution need not wait until the creation of a policy: messages can begin to be stored immediately with no retention decisions made for a number of years.

Education and Training

Do not under estimate the importance of education and training all users. Regardless of tenure within the organization, all staff must be informed about the new record retention policies being developed and what effort they must put in to ensure compliance. Users must also be trained on how to use the archiving solution and how to manage any retention exceptions.

Audit

Part of the training should also include awareness of the auditing programs that will report on their effectiveness and the penalties for noncompliance. Long after the policy and technical systems are in place, the core team will continue the process of education and auditing. They must also make sure that any changes to the technical environment, or business and legal requirements, are reflected in the record retention policy.

Implementing Your New Policies

Getting Help

With many different archiving software solutions on the market, and many ways to implement them, it can be beneficial to seek out the experience of a consultant or integrator to help put e-mail archiving policies into practice. Consider whether you have the time and

experience required to conduct an assessment of archiving needs, develop a retention policy and schedule, plan and implement an archiving product, and train and audit the solution. The software or hardware vendor may be able to recommend an appropriate consulting solution for your needs.

Using Enterprise Vault

Symantec's popular Enterprise Vault package can be used to automate email retention as discussed above. The system supports integration into multiple email platforms, including Microsoft Exchange and Lotus Domino. Enterprise Vault integrates with the email servers and clients (e.g. Outlook or Lotus Notes). This integration both simplifies user access to messages and allows users to place messages in special retention folders as needed. Administrators have the ability to assign archive folders to users as well as set custom filters using advanced criteria to assign retention exceptions to special content.

The advantages of Enterprise Vault allow administrators begin with a basic blanket policy for most messages. As discussed above, this policy would apply to nearly all messages in the system, but exceptions could be dealt with in one of two ways. The most common implementation includes folder-driven archiving. This is accomplished by having IT push out folders to the user inbox inline with the retention policy. For example, you may have three retention folders created for each user with different categories and retention rules (e.g. Business Records -5yrs; Legal Records - 7yrs; Financial Records -10yrs). Folder-driven archiving enables custom managed folders to which users can move email records with the different requirements. Additionally implementations further enhance classification efforts via custom filters for messages from specific users, such as HR or finance, to extend the protection of these critical communications. Although these techniques will suffice for most cases, some administrators might want to explore the capabilities of custom filters beyond the user or department level, searching on other message metadata and even content. Messages are generally recovered by users as needed, but the archive explorer interface also allows administrators to search for specific content across all users if needed.

If litigation-related discovery is needed, the archive can be explored with the optional Discovery Accelerator module. This module allows designated individuals to execute search queries against the contents of the entire archive in order to produce messages which are determined to be relevant. These searches include message metadata and content, and may relate to specific custodians, usage patterns, and keywords. Discovery accelerator includes a robust litigation hold capability that can be applied to the messages included in the overall search result set. Enabling litigation hold on the contents of the search result set will prevent the archive from deleting this content pursuant to the ongoing execution of the message disposition schedule. The search, review, and preservation workflow of Discovery Accelerator is fully audited and provides a powerful way to respond to legal issues related to email.

Conclusion

There is no universal solution for the puzzle of e-mail retention or destruction. Laws and regulations are no more clear than internal needs when it comes to deciding how long to keep e-mail messages. Each organization must take a look at the different types of corporate data contained within their e-mail system and develop a policy and schedule to retain and delete messages. Although the answers will vary, each organization should focus on creating a simple and sensible e-mail retention policy.

With e-mail becoming increasingly critical to businesses, interest in e-mail content and handling processes among the legal community was inevitable. No organization can afford to be without a retention policy for e-mail, since this omission could open them to serious penalties from the regulators and litigators.

Although the creation of an overall e-mail retention policy can be complex and time consuming, implementation of an email-archiving system need not wait for it to be completed. In fact, it can be simpler and less risky to simply start collecting all email records immediately rather than trying to create a perfect system and failing. Setting up an archiving solution such as Enterprise Vault prior to the creation of a retention policy may also speed up the policy creation and enforcement process by enabling flexible automated and manual retention methods that would otherwise not be available. Often the best first steps in initiating an email retention policy program are to select an email archiving application compatible with your existing email system and begin archiving all messages without committing to any deletion schedule.

About Contoural, Inc.

Contoural is a leading independent provider of business and technology consulting services focused on litigation readiness, compliance, information and records management, and data-storage strategy. Contoural helps clients address the business requirements emerging around data. For example, electronic discovery rules—under the new Federal Rules of Civil Procedure—now require US companies entering litigation to know what electronically stored information they have, where the ESI is stored, and how quickly they can retrieve that ESI. Similar issues and requirements affect business records in many countries worldwide.

Similarly, legal and regulatory compliance requirements under emerging privacy laws are motivating enterprises to take a closer look at the integrity and security of electronic document files and other digital data. Contoural helps clients understand the business requirements for managing records, and then assists clients to align these business needs with their IT strategies and storage spending. These services bridge the gap between applications and data storage.

Contoural services include:

- Records-retention policy development
- Litigation-discovery process improvement
- Data classification and storage strategy
- Data archiving solution design

With these services, Contoural helps enterprises ensure compliance and reduce risks, while also achieving litigation readiness and reducing costs.

Contoural, Inc.
1935 Landings Drive
Mountain View, CA 94043
650-390-0800
www.Contoural.com
info@contoural.com

About Symantec Enterprise Vault

Symantec Enterprise Vault™ provides a software-based intelligent archiving platform that stores, manages and enables discovery of corporate data from email systems, file server environments, instant messaging platforms, and content management and collaboration systems. Because not all data is created equally, Enterprise Vault utilizes intelligent classification and retention technologies to capture, categorize, index and store target data in order to enforce policies and protect corporate assets while reducing storage costs and simplifying management. Enterprise Vault also provides specialized applications, such as Discovery Accelerator and Compliance Accelerator, that mine archived data to support legal discovery, content compliance, knowledge management, and information security initiatives.

Discovery Accelerator extends the basic search functionality of Enterprise Vault to help lower the cost of data collection and facilitate the search and recovery process of archived items used for electronic discovery. Discovery Accelerator further supports the new Federal Rules of Civil Procedure through configurable enforcement of items during a litigation holds and flexible export capabilities to simplify production. Enterprise Vault is deployed at more than 6000 customers to provide storage management and E-Discovery solutions for more than 8 million mailboxes.

To learn more about how Enterprise Vault and Discovery Accelerator can help IT organizations prepare for the Federal Rules and for the next E-Discovery request please visit www.symantec.com/enterprisevault.