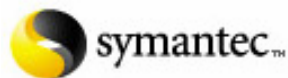




CIO's Guide to the New Federal Rules of Civil Procedure

Assessing the IT Impact of Email / File Retention and Discovery Requirements

Sponsored by:
Symantec Inc.



contoural 

1935 Landings Drive
Mountain View, California
650 390-0800
www.contoural.com

Table of Contents

	<u>Page</u>
Executive Summary	3
Introduction – Are You Ready?	3
■ Self Assessment	
Federal Rules of Civil Procedure – Overview	4
■ What are the Federal Rules of Civil Procedure?	
■ Who is affected by the FRCP changes?	
■ Understanding the New Rules	
■ How do these changes impact IT?	
Building an Action Plan to Enhance Litigation Readiness under the FRCP	7
■ Engage key stakeholders	
■ Create/update a record retention policy and schedule	
■ Review/update your litigation hold policies and procedures	
■ Implement appropriate technology solutions	
■ Employee training & audit	
Examining FRCP Best Practice Scenarios	9
FRCP Case Studies:	10
■ Large Manufacturing Company	
■ Large Bank	
■ Mid-sized Technology Company	
Summary	15

Please Note: This paper is provided for general informational purposes and is not legal advice. If you require legal advice for your specific circumstances, please consult with a competent attorney licensed to practice in your jurisdiction.

Executive Summary

Litigation readiness has become an increasingly important IT responsibility, often forging new but necessary links between IT and legal staffs. In today's business environment, the scope of IT's role must expand to incorporate e-discovery requirements. Recent amendments to the Federal Rules of Civil Procedure (FRCP) mandate changes in the way organizations manage their data. IT needs to have a detailed knowledge of what information is kept, where data is stored, and how long to keep it. Also, IT needs to have the ability to quickly and accurately respond to litigation hold notices. Establishing the correct processes and procedures around data retention, implementing automated solutions to ensure compliance, improving search and retrieval speed, as well as increasing user productivity, could ultimately save most companies millions of dollars.

Introduction – Are You Ready?

Legal and regulatory compliance requirements are changing the rules for electronic records retention and storage. Changes in laws and regulations can impact what types of business records you create and retain, how securely those records must be stored and protected, how long they must be kept, and how quickly they must be retrieved when required. Certain industry segments such as banking, financial services and healthcare have been subject to more stringent regulations and have developed data management policies and procedures. Litigation risks and associated costs are stronger drivers than regulatory compliance for many firms, particularly in the US. Moreover, recent amendments to the FRCP were issued to refine and clarify the e-discovery requirements for electronically stored information (ESI). The new rules are causing companies to question their current practice in the context of litigation readiness.

Self Assessment:

Does your enterprise have the necessary policies and solutions in place to meet these new requirements? Take a moment and evaluate your department's readiness if asked to support a litigation request tomorrow. Identifying any potential weaknesses or missing processes or skills should underscore areas of risk and the need to plan accordingly. To understand your potential level of risk, ask yourself the following questions:

- Do you have an up-to-date record retention policy and schedule?
- Is your record retention policy enforced and audited for compliance?
- Can you implement a litigation hold and cost-effectively sustain it for a period of time? How about multiple, overlapping holds?
- Can you easily discover email, files and other electronic documents across the organization, including laptops and remote offices?
- Can you complete your discovery within days or weeks?
- Can you be certain that you have found everything during your discovery?
- Can you provide all electronic documents in their original format if required?
- Can you (and your legal counsel) easily and effectively review all discovered documents to produce a smaller set suitable for review by outside counsel?

Federal Rules of Civil Procedure Overview

What are the Federal Rules of Civil Procedure?

The FRCP defines a uniform set of requirements and more predictable court procedures for trying civil suits in a consistent manner and reducing the costs, delays and risks. It is important to note that in addition to the U.S. federal courts, many states also base their rules for civil trials on the FRCP. Recently enacted amendments to the FRCP attempt to address the current business environment in which the vast majority of information, including email, is created and stored in electronic format. The new rules for discovery and disclosure of electronically stored information (ESI) in court procedures require data to be produced in a timely and complete manner.

Who is affected by the FRCP changes?

Unlike industry specific regulatory requirements (such as the SEC and NASD rules for broker-dealers and financial institutions), the FRCP has a very broad scope. Any company, public or private, that is subject to litigation will be impacted. Public sector entities are included as well. These requirements will have a significant impact on corporate record management policies and IT's ability to execute and enforce those policies for electronic records and information.

The Problem with Back Up

In the context of e-discovery, back up tapes can be extremely problematic. Back up procedures are intended to provide insurance for data loss. Finding specific information on tape can be time consuming and costly. Information contained on back up tapes should not be considered a substitute for an information archive. Also, back up data may be incomplete as recent items may be deleted before the next scheduled back up.

Understanding the New Rules

The FRCP rules are relatively long and complex. The following list provides a high-level summary of the key provisions that directly impact how your organization manages ESI and the discovery process. For complete text of the FRCP, please visit <http://www.law.cornell.edu/rules/frcp/>.

- *Rule 16: Pretrial Conferences:* Requires opposing parties to meet and discuss a discovery plan and evaluate the protection and production of electronic data.
- *Rule 26(a): Initial disclosure of sources of discoverable information:* Parties must identify all sources of electronic information that may be relevant by category and location.
- *Rule 26(b)(2): Initial disclosure of information that is not discoverable due to undue burden or cost:* The amendment clarifies that ESI may not have to be produced from sources that are not reasonably accessible such as information stored on backup tapes or on obsolete legacy systems. The responding party must identify the sources of potentially responsive information that were excluded due to the burden or costs of accessing the information. Caution: The interpretation of this phrase may vary. Undue burden must be proved and does not mean the information is not discoverable.
- *Rule 26(b)(5) Privileged information:* If privileged information is inadvertently given to the opposing party, the recipient must return or destroy the information.
- *Rule 26(f): Early Discussion Preparedness:* The opposing parties must meet and discuss what systems ESI may reside upon, along with other potential data sources, if those sources may be regarded as reasonably accessible. This “meet and confer” process should also address the form in which the information is to be produced and the preservation of the information through the litigation hold process.
- *Rule 34(a): Email is Discoverable:* Email is a form of ESI and is discoverable.
- *Rule 34(b): Form of Production:* As part of the discovery process, ESI may be produced in a form which is it is “ordinarily maintained” or in a form that is “reasonably usable” unless otherwise requested.
- *Rule 37(f): Safe Harbor:* This rule provides a company with limited protection from sanctions when it is unable to provide ESI due to the routine or good faith operation of automated record destruction policies and procedures.

How do these changes impact IT?

While the amendments to the FRCP present significant challenges to legal counsel, fulfilling the requirements will most certainly impact the IT organization and become an increasingly large cost and resource issue. Like it or not, more CIOs and IT managers will need to become e-discovery experts. Table 1 lists IT tasks and capabilities that will be vital in supporting e-discovery requirements.

Table 1
FRCP Amendments: The Rules & IT Responsibilities

E-Discovery Process	Litigation Hold	Data Collection & Processing	Data Review & Production
Rule 16: Pretrial Conferences	Develop/review/update all Litigation Hold Policies and Procedures	Create a discovery plan - Where is all the relevant data? How long will it take to collect the data?	
	Demonstrate the ability to enforce a Litigation Hold Notice	Discovery plan - Where is the data? How long will it take to collect the data?	
	Freeze back up tape recycling	What about metadata?	
Rule 26(a): Initial disclosure of sources of information		Identify all sources of ESI that may be relevant; Index and classify all ESI for rapid search and retrieval.	
Rule 26(b) (2): Disclosure of information that is not discoverable due to undue burden or cost		Be able to prove the costs and time required to produce the requested ESI; For instance, the cost of restoring back up tapes or legacy data. Understand if these potential sources contain relevant data.	
Rule 26(b)(5): Privileged Information		Tag all privileged information so it is not given to the opposing party; Search discoverable information for anything that might be privileged and was inadvertently given to opposing party.	
		Find and return or destroy information from opposing party when necessary.	
Rule 26(f) Early Discussion Preparedness	Discuss record retention policies and technologies used for data preservation through the litigation hold process to prevent spoliation; Document chain of custody procedures and authentication.	Provide sources ESI resides on along with any other data sources; Evaluate ESI source accessibility.	Address the form in which the data will be produced - (PST, pdf, tiff, jpeg)
Rule 34(a): Email is discoverable	Ability to enforce a litigation hold on all email to prevent deletion by users or by automation solutions.	Ability to search and find all relevant email and attachments - on all potential sources including servers, desktops, laptops, PSTs; Back up tapes only provide a snapshot of data - How can you find data generated or deleted between backups?	Review only what is relevant as quickly as possible.
Rule 34(b): Form of Production			ESI may be produced in the form which it is ordinarily maintained unless otherwise requested

Building an Action Plan to Enhance Litigation Readiness under the FRCP

The new rules raise the bar for information and storage management. In general, an effective strategy will require improved records-management processes and infrastructure, combined with technology solutions for search and discovery. There are a number of steps an organization can take to minimize risk and prepare for litigation.

1) Engage Key Stakeholders:

To help ensure the success of any litigation readiness initiative, form a steering committee of key stakeholders. The steering committee should consist of members from in-house legal counsel, outside legal counsel, IT operations, HR and finance managers, compliance officers, records managers, and key individuals from operational business units. While litigation readiness may be a crucial business driver for the organization, understanding all the potential business drivers is necessary in developing the appropriate policies and effective procedures.

2) Create or Update a Document Record Retention Policy and Schedule:

New requirements such as the FRCP, litigation readiness strategies as well as operational business needs should be reflected in up-to-date policies and procedures for record retention and destruction. For most organizations, semi-structured data and unstructured data represent the biggest pain points in terms of finding and managing data to meet e-discovery requirements. As Figure 1 illustrates, many companies see semi-structured data, especially email, as the most immediate pain point that they need to address to reduce the risks and costs of e-discovery. Unstructured data historically has been viewed as a huge storage-cost problem. However, addressing files has become an increasingly important driver in litigation readiness.

Figure 1
Business Drivers for Data Management

		BUSINESS NEEDS		
		Compliance, Discovery	Application Performance	Storage Cost
DATA TYPES				
Semi-structured: E-mail, Check Imaging		+++	+	++
Structured: Databases, ERP, CRM		+	+++	++
Unstructured: Office Docs, Audio Files		++	+	+++

Source: Contoural Inc.

3) Review/Update your Litigation Hold Policy & Procedures:

The key to addressing the Rule 37 “good faith” concept is demonstrating an organization has the proper policies and procedures in place to quickly and reliably implement litigation holds on its data and ensuring that data will not be destroyed due to a routine or automated process.

4) Implement Appropriate Technology Solutions:

Many of the challenges faced in achieving litigation readiness can be traced to management of electronic data. The exploding volume of email and attachments as well as shared files need to be managed in a way that they can be captured and produced when needed as well as deleted according to the company's retention schedule. Since many email records and files are duplicated throughout an organization, increased operational efficiencies and significant cost savings can be often be achieved through de-duplication. Email archiving and file system archiving solutions can help organizations achieve their objectives for litigation readiness, (including FRCP requirements), operational cost savings and regulatory compliance.

Litigation Readiness:

- Effective archiving solutions can reduce or eliminate the need to search for email messages on backup tapes and in PST files, and can also reduce or eliminate duplicate documents that must be reviewed by counsel.
- Archiving can automate the collection, processing and review of the target information contained in the archives.
- Tools enable email and attachments to be quickly searched, tracked, filtered and marked for counsel review or production.

Operational Business Needs:

- Email archiving can eliminate quotas and provide transparent user access to archived data delivering measurable increases in employee productivity.
- Archiving solutions reduce storage costs of unstructured data by keeping only the files that are necessary and decreasing the duplication of files.
- File system archiving can automatically archive electronic files placed on share drives to a centrally managed archiving system. Centrally managed policies can eliminate duplicate files, protect files from premature deletion, index files for fast retrieval, and reduce storage costs by better managing storage requirements over time.

Regulatory Compliance:

- Archiving solutions can provide automatic capture of e-mail messages and attachments, reducing dependence on user behavior to maintain a complete business record.
- Archiving solutions can provide tools to help classify the content of email and files and apply the appropriate retention periods.
- Automated enforcement of retention and deletion rules allows for consistent and efficient policy compliance.

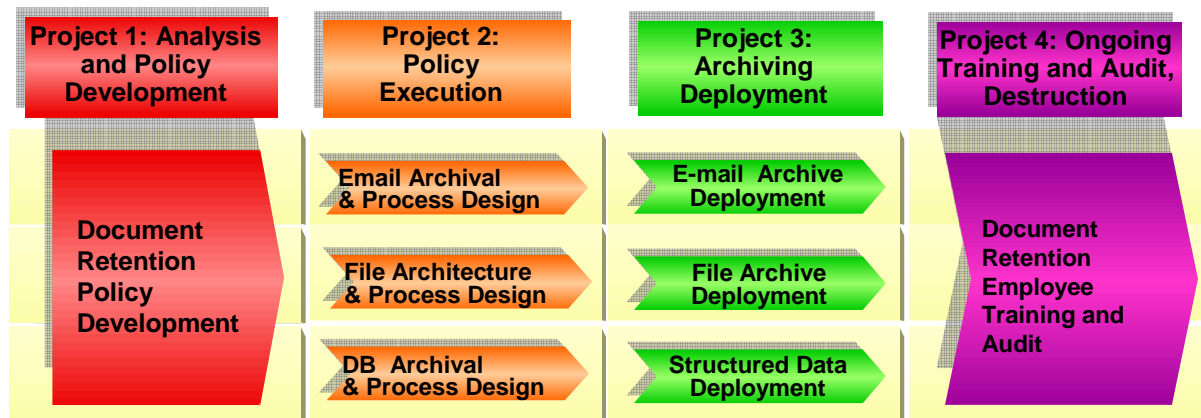
5) Employee Training & Audit:

Employees need to be educated on all new policies and procedures as well as any new email archive solutions. And, it is important to be able to show that employees have been trained in the policy and the retention tools/procedures made available to them.

- Maintain documented procedures for training new employees as well as existing employees.
- Maintain audit or certification logs of employee policy exposure and training, with employee sign-off that policies have been read and understood.
- Have procedures for periodic (usually annually) refresh of employee certification.
- Make policies readily available to employees on the corporate intranet.
- Maintain computer-based training on any records management tools implemented for employee use.

Figure 2 illustrates a phased approach to an organized, comprehensive IT project plan for email and electronic file archiving. Because the new FRCP rules are unclear on exactly what is reasonably and unreasonably accessible data (Rule 26(b)) a company's ability to demonstrate its record policy and consistent, repetitive and verifiable enforcement will be subject to increased scrutiny. Using technology to automate records management enables consistent enforcement without having to rely on human behavior. This is particularly important for high volume electronic records such as email and attached files.

Figure 2
Comprehensive Archiving Project Plan



Source: Contoural Inc.

Examining FRCP Best Practice Scenarios

Implementing Archiving as Part of Your Litigation Readiness Strategy

There are many archiving solution vendors in today's market. These solutions offer a variety of features and functions. This is still a relatively new market and products continue to evolve and add new capabilities in response to changing business requirements. In general, archiving solutions provide a 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. Organizations can implement archiving in either an in-house or outsourced model. Smaller companies with fewer IT resources may choose to use the outsourced model.

Archiving Case Studies

The following three case studies provide examples of business challenges and solutions around litigation readiness and storage management. Contoural has developed these case studies in collaboration with Symantec, based on experience with actual client organizations, and are meant to provide examples of typical business cases. The company profiles vary by industry, enterprise size and business drivers. They include examples of a large manufacturing company, a large, regulated banking enterprise and a mid-sized technology company. In each case, the organization uses archiving technology as part of its overall solution set.

FRCP Case Study – Large Manufacturing Company

Improving litigation readiness while reducing overall storage costs

Profile

XYZ Company is a large international organization that designs, develops, manufactures and markets a broad range of products directly and through joint ventures. The company has operations in more than 30 countries around the world, employs 50,000 people and has revenues in excess of \$20 billion. With over 600 patents, the company is also a leader in innovation.

Business & IT Challenges

While not operating in a heavily regulated industry, the company wanted to mitigate possible future risk by making sure its corporate governance policies were in line with industry best practices. The main business drivers were litigation readiness and operational needs (reducing overall storage costs). The company needed to address its outdated data retention policy that was not consistently enforced, and its escalating e-discovery costs. The company's increasing email and file-system storage costs reflected the fact that – as a design and development company – the majority of email correspondence included large attachments of drawings, photos or other types of graphics. The problem was compounded by the number of duplicate copies sent via email and copies saved on shared file drives.

Discovery challenges

- History of patent, IP and employment lawsuits – 100 cases per year and growing 15% annually
- Must ensure data integrity and preservation
- Reliance on outside consultants for data collection and processing
- Manual and time-consuming litigation hold process
- High IT costs and delays due to restoring historical data from back up tapes
- Concerns regarding redundant storage from restoration
- Lack of central data repository for searching and tagging potentially responsive records

Environment

- 50,000 users – Microsoft Exchange, Windows file servers
- Heavy volume of encrypted messages
- 70 TB of historical data across backups, PSTs & file shares
- Global data centers

Solution

The company used a phased approach to analyzing and understanding the issues. During the first phase, updates to the record retention policy and scheduled ensured all record types and retention periods were correct. Since the company had a “save everything” corporate culture, changing employee behavior to comply with the new policy and schedule would prove difficult. Automating the records management process, as much as possible, would be critical for success.

During the second phase, Contoural evaluated automation solutions and helped with deployment plans for email and file system archiving. The evaluation process began with defining solution requirements in terms of functionality and performance, as well as putting together initial cost estimates. Including functional requirements for litigation support was an important component of the overall requirements. The top three vendors that met the initial set of requirements began a detailed RFP process – including RFP responses, vendor presentations and reference checks with customers of similar size and business needs. After selecting an in-house email and file system archiving solution, the company conducted a pilot installation, followed by a phased implementation rolled out by region over a 1-year period.

Finally, updates to the company's litigation hold policy and procedures ensured appropriate preservation of archived messages and files in the event of litigation. According to this organization's general counsel, "We needed to make sure we have a repeatable and consistent process for enforcing litigation holds." The discovery module of the selected archiving solution supports the litigation hold process, enabling fast searching of the archive.

IT Archiving Policies & Procedures

- Implemented batch processing to meet data privacy requirements in Europe.
- Deployed mailbox archiving based on 70% of quota and anything over 14 days old.
- Automatically clear out the Deleted Items folder once per week.
- All email kept for 3 years in accordance with the record retention policy.
- Identified key executives and departments for exceptions to the standard three year retention and assign appropriate retention periods (most records for these individuals will be saved indefinitely).
- Migrated PSTs into the archive and enacted an end user policy preventing PST creation.
- Offline email use supported through mailbox synchronization service.
- Periodic audits of file shares and C drives to detect and report on PST existence.
- Data migrated to secondary storage after 90 days.
- Litigation hold capabilities implemented. A litigation hold imposes a hold on all email based on selection criteria such as names, dates within a give time frame, and key words. Once litigation hold is removed, emails revert to their original deletion date.

Results

- The updated record retention policy and schedule now provide a complete inventory of record types including electronic records.
- Single-instance storage and compression reduced storage costs by 40% or \$330,000.
- Decreased backup time by 30%.
- Reduced IT and help desk calls on email administrative tasks, for an approximate labor savings of \$90,000.
- Eliminated reliance on outside vendors for data collection, forensic services and costs of over \$250,000 per year.
- Automated mailbox management ensures compliance by automatically deleting records in accordance with the policy and retention schedule and increased user productivity by eliminating user's manual response to mailbox quotas.
- Provided intelligent archiving for legal and automated litigation hold enforcement.
- Enabled legal staff to search and extract data from the archive without IT assistance.
- Fast access for end users, even for those in remote offices.

FRCP Case Study – Large Bank

Bank deploys email archiving for legal discovery

Profile

ABC Bank is a U.S. based, full-service commercial bank, providing a broad mix of financial services to businesses and individuals. The bank's markets include consumers, small and medium businesses, real estate, and trade finance. The bank also offers investment and financial management, trust services, private banking, insurance services, and global custody services. The bank currently employs more than 15,000 people.

Business Challenge

As part of the highly-regulated financial services industry, the bank had a records retention policy that focused on laws and regulations such as SEC Rule 17a-4, NASD 3010/3100, Sarbanes Oxley, the Financial Services and Markets Act 2000 and many others. At the time the policy was previously updated, the focus had been primarily on the management of paper records. Realizing that email is now a crucial form of legal evidence, the Bank needed to update its policy and practices to address electronically stored information (ESI) as called out in the FRCP amendments.

The bank also needed to update its email archiving solution, which did not support the legal department's e-discovery objectives. In addition, the IT department wanted to address general storage management issues such as reducing back up windows and supporting disaster recovery plans. The bank had previously deployed a leading archiving solution, but was unhappy with its ability to meet e-discovery requests as well as other deployment issues.

Discovery challenges

- Regulatory investigation – 30 day action required
- Required to save email for 7 years
- Must capture all meta data for email
- Risk of not finding and producing everything

Environment

- 15,000 users - Microsoft Exchange
- 30 TB of Exchange backup tapes
- Heavy volume of encrypted messages
- Multiple sites
- Disparate systems due to mergers and acquisitions

Solution

In evaluating new alternatives, the bank's IT department was charged with finding a solution that would provide: 1) Full data capture of all email and related information including calendars, contacts and tasks; 2) Simple integration with the existing Exchange servers; 3) Easy scalability; 4) Complete transparency to the end users. The company looked at all the leading email archiving solutions during the review process.

The bank ultimately selected Symantec's Enterprise Vault. The primary differentiator was Symantec's ability to provide direct integration with WORM storage, full data capture using journaling, and an integrated compliance supervision solution using Compliance Accelerator. Enterprise Vault also fit seamlessly into their production environment with no disruption to end users. "Not having to re-architect the Exchange environment was a huge benefit," said the CIO.

Today, the bank has over 10,000 mailboxes under archive. Deployment is being rolled out by management level in accordance with the company's legal objectives. Within the next three to six months, the entire company will be covered by the archive -- approximately 15,000 mailboxes. No formal employee training has been necessary, as the Enterprise Vault solution is completely transparent to the end users.

The bank is utilizing mailbox management stubbing, compression and single-instance storage capabilities of the Symantec solution. The parameters of email messages being archived include the Header, Message Body, and Attachments. PSTs are being archived simultaneously as end users are brought up on the archive.

IT Archiving Policies & Procedures

- Enabled journaling to capture all email correspondence and attachments.
- Captured distribution list contents and blind copies, to provide a full audit record communications receipt.
- Deployed mailbox archiving based on 70% of quota.
- All email kept for 7 years in accordance with the record retention policy.
- Migrate files to secondary storage after 180 days.
- Migrated PSTs into the archive and enacted an end user policy preventing PST creation.
- Offline access solution in place of PSTs, as in previous case study.

Results

- Policy and schedule updated to meet new litigation readiness and compliance needs.
- Automated message management and deletion is completely transparent to end users.
- Elimination of PST files.
- Fast and easy searching.
- Reduced e-discovery response time for email from 3 months to 24 hours
- Saved \$200,000 per year in IT labor costs for restoring tapes and finding data on PSTs.
- 70% faster backups than previous solution.
- Easy to perform compliance audits.
- Reduced risk of fines for incomplete or faulty discovery requests.

FRCP Case Study – Mid-Sized Technology Company

Semiconductor Company gets employees out of “email jail” and realizes improved storage operations

Profile

This mid-sized enterprise is a provider of semiconductors for wired and wireless communications. The company has a broad portfolio of system-on-a-chip and software solutions that it sells to manufacturers of computing, networking equipment, digital entertainment and broadband access products. Headquartered in California, the company employs approximately 5,000 people worldwide.

Business Challenge

The initial business driver for the company to choose an email archiving system came from the in-house IT department. With a save-everything, engineering-centric corporate culture, email mailboxes had no quotas. When the company decided to migrate from Notes to an Exchange environment, quotas needed to be put into place to manage storage costs. Each person was given a large 1GB mailbox. According to the company’s IT Manager, “that’s really big by industry standards but it turns out the mailboxes weren’t big enough.” IT quickly became overwhelmed with Help Desk calls on “Email Jail” issues and scrambled to get “extremely large emergency attachments” sent out.

Other issues:

Email Management

- Email storage costs growing exponentially
- Increasing IT costs for managing email support
- End user frustration and productivity loss due to quotas

Future Discovery challenges

- Frequent employment claims
- Reduce time to find data
- Searching and indexing data
- High IT cost and delay on restoring historical data - tapes, PSTs and laptops
- Policy enforcement risk (quotas, PSTs)

Environment

- 5,000 Users - Microsoft Exchange
- 35 TB of historical data across backups and PSTs

Solution

In evaluating alternatives, the company first turned to Gartner Group’s Magic Quadrant report on email archiving. IT selected the top two vendors to evaluate. Each vendor was evaluated on paper for specific technical requirements, functionality and support. Next, each vendor came in for demonstrations. IT then proceeded with a 30-day trail in which the software was installed and tested. When testing was complete, further considerations of price and support were added. “It was a difficult choice. One vendor had a lot of good features but at the time couldn’t offer Off-Line Vault which we needed for our remote sites.” The company chose Symantec’s Enterprise Vault solution. Features include e-discovery, migrating PSTs and mailbox management. Off-Line Vault is the most important feature for supporting this company’s global operations.

Today, the company has 4,000 mailboxes under archive. All employees’ emails are now being archived. The system was deployed mailbox-by-mailbox on the servers, at a rate of about 80 people per day. End user deployment was simple and cost effective due to the characteristics of the solution chosen. End users received an email about the system and a link to a Help Desk FAQ document as they were deployed. There have been no end users problems to date.

Future Legal Business Drivers:

The Company's legal department has now become more interested in how all email is archived and is looking at adding Legal Discovery and Compliance solution modules to the archive in Phase 2 to support recent changes in regulations and requirements.

IT Archiving Policies & Procedures

- User driven archiving policy; end users classify data in a limited number of pre-set folders (e.g., business, personal, HR).
- Deployed folder archiving based on 70% of quota and anything over 21 days old
- Automatically clear out Deleted Items folder once per week
- All email kept for two years in accordance with the record retention policy
- Applied default policy using automated classification for other groups, such as sales, which need to retain email for three years.
- Migrated PSTs into the archive and enacted an end user policy preventing PST creation
- Data migrated to secondary storage after 180 days

Results

- Automated mailbox management reduced IT support cost by \$95,000 per year
- Eliminated user quotas and increased employee productivity; employees still need to classify email into appropriate folders but no longer have quota restrictions
- Transparent user access to the archive
- 45% reduction in email maintenance costs
- 50% reduction expected in the amount of storage needed for Exchange servers
- Decreased back-up time by 25%
- Easy migration from Notes to Exchange environment
- Provided platform to enhance litigation readiness in the future

Summary

Managing an ever increasing volume of electronic data is now a business imperative. Corporate executives, legal counsel and IT managers must work together to define the requirements for policies and solutions to meet this challenging business environment. To meet the new FRCP amendments as well as evolving regulatory requirements, organizations should implement technologies such as email and file-system archiving solutions that can capture data, retain it in compliance with retention policies, and produce information in a timely manner. The recent FRCP amendments emphasize the importance of being prepared for litigation. Here are some ways to see if your organization is ready:

Checklist for FRCP Readiness Evaluation

- Do you have an up-to-date record retention policy and schedule?
- Is your record retention policy enforced and audited for compliance?
- Can you implement a litigation hold and cost-effectively sustain it for a period of time? How about multiple, overlapping holds?
- Can you easily discover email, files and other electronic documents across the organization, including laptops and remote offices?
- Can you complete your discovery within days or weeks?
- Can you be certain that you have found everything during your discovery?
- Can you provide all electronic documents in their original format if required?
- Can you (and your legal counsel) easily and effectively review all discovered documents to produce a smaller set suitable for review by outside counsel?

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 5000 customers to provide storage management and E-Discovery solutions for 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.

About Contoural, Inc.

Contoural is a leading independent provider of business and technology consulting services focused on compliance, intelligent data management and storage strategy. Contoural helps clients address the emerging business requirements around data, and then to align their business needs with IT strategy and storage spending. This bridges the gap between applications and storage. Contoural helps enterprises ensure compliance and reduce risks, while also optimizing service levels and reducing costs.

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