

"The Dog Ate My Homework..."

...and Other Poor Excuses for Not Archiving

By Sean Regan, Product Marketing Manager, Symantec

At first glance, the recent survey on email archiving by the Storage Networking Industry Association (SNIA) seems to contradict itself. It found that while most companies realize they have to retain email and other electronic records for at least 50 years, most admit they are "highly dissatisfied" with their archiving policies. The consequences for not properly retaining e-records are severe, and can be avoided by implementing a software-based email archiving system. So why hasn't your company done so already? Working with customers across all industries, Symantec has identified a handful of excuses companies most often use when explaining why they have not established an archiving policy. The common thread running through all of these excuses is that none of them is valid, and can place a company at enormous risk of litigation, fines and damage to their reputations and customer relationships.

An email archiving system is more than a collection of backup tapes. Email archiving software automatically moves email messages and attachments from email servers such as Microsoft Exchange and

Lotus Notes based on corporate policies or rules to a central repository. Records are indexed so they are easy to find and recover. Records are retained for the appropriate period of time according to internal policies, external regulatory requirements or both, and an audit trail is provided that shows who accessed any email and when.

Federal Rules of Civil Procedure

Being sued is part of doing business, and being able to find subpoenaed email records is critical to defending your organization. In December, 2006, the Federal Rules of Civil Procedure (FRCP) were amended to refine and clarify the e-discovery requirements for electronically stored information, placing the responsibility of producing subpoenaed email records on the defendant, not regulators or the plaintiff. 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 US federal courts, many states also base their rules for civil trials on the FRCP. The December, 2006, amendments 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 in court procedures require data to be produced in a timely and complete manner.

The burden of preserving emails and producing specific records for presentation in court typically falls on the IT department's shoulders, and recovering emails is an extremely time-consuming and expensive process. According to research conducted by analyst firm Gartner, the average cost of defending a lawsuit exceeds \$1.5 million per case, with 20% to 30% of that being internal and mostly IT-related. But that cost pales in comparison to the sanctions a judge could hand down if a company is unable to preserve and produce relevant emails.

Despite the fact that the consequences of not properly retaining and managing email records are severe, and companies are aware of those consequences, the majority have not developed and implemented a system for retaining email records over the long term. The August, 2007, SNIA survey, entitled the "SNIA 100-Year Archive Requirements Survey Report," found that 80% of respondents have information they must keep for more than 50 years, and 68% say they must keep some types of information for more than 100 years. Overall, those surveyed reported their current archiving practices are too manual, prone to error, costly and lack coordination across the organization. Seventy percent said they are "highly dissatisfied" with their ability to retrieve and read information in 50 years. The SNIA surveyed IT professionals from 276 organizations.

Top Five Considerations for Choosing an Archiving Technology

Selecting an archiving solution for email and other vital business data can seem like a daunting task. By definition, archiving is a long-term proposition, so it's important to evaluate the available products thoroughly before making a decision. Keeping a few basic principles in mind can help you with that process. Here are five recommendations for choosing an archiving technology:

1. Think long term. Be sure to select an archiving product that is flexible enough to support changes in your business and computing environment. Your chosen solution should be able to maintain and enhance performance levels when you add users, data and applications.

2. Consider manageability. IT organizations are demanding manageability from archives similar to what they get from other infrastructure applications. Secure, role-based administration and granular provisioning and reporting are the foundations of a good archiving solution.

3. Focus on content intelligence. Because not all information is created equal, organizations need to manage and retain different pieces of information based on their individual value. Certain content (such as orders and contracts) may need to be maintained for years, while other data (such as personal email and newsletters) can be eliminated more quickly.

4. Optimize your total cost of ownership. While email archives often provide a quick return on investment from storage savings, a good solution also provides technical and administrative functionality that helps lower the cost of administration and overall ownership of the archive.

5. Look for best-of-breed, open solutions. Your archiving platform should be able to grow and integrate with other systems as your environment changes and expands. It must provide open application programming interfaces (APIs) and broad support for long-term storage, as well as for structured and unstructured data besides email.

Store, Manage and Discover

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



Poor Excuses

"We keep everything."

One common excuse companies rely on for why they do not have an archiving system in place is that they simply save every single email and attachment that comes into or flows out of the company's email servers, regularly dumping older records onto backup tapes. But in the context of e-discovery, backup tapes can be extremely problematic. Backup procedures are intended to provide insurance for data loss. Finding specific information on tape can be time-consuming and costly. Information contained on backup tapes should not be considered a substitute for an information archive. Also, backup data may be incomplete as recent items may be deleted before the next scheduled backup.

On the other extreme, many organizations simply delete everything after a certain time period, such as 30 days or three months. This is simply not a defensible process, particularly in light of the FRCP amendments that took effect in December, 2006.

"Archiving is too costly."

CEOs across all industries are under constant pressure to cut costs, and the IT department's budget is usually the first on the chopping block. IT is being asked to do more with less money, and a valid concern is that archiving will require too much storage and opens the organization to e-discovery risk.

Wrong. Archiving provides storage optimization and infrastructure benefits. Implementing an archive also reduces e-discovery risk by establishing mechanisms for the automated retention, preservation and expiration of archived content according to policy, avoiding judgments related to spoliation. Also, remember: the cost of implementing and managing email archiving software pales in comparison to the sanctions a judge might hand down for improper email retention or the cost of reviewing massive amounts of data on backup tapes.

"We need more time to define our archiving policy."

In some cases, an organization has decided to implement an email archiving system, but can't come to an agreement internally on whose email should be archived and for how long. Spending a year to define a policy and then another year to select, buy and implement technology is a recipe for disaster. You need to preserve data related to litigation today. You need to

"Being sued is part of doing business, and being able to find subpoenaed email records is critical to defending your organization."

know what you have and where it is located today. There's nothing wrong with regularly revisiting your archiving policies and revising them as internal and external requirements evolve. In the short term, establish a broad policy that meets the applicable requirements of external laws and regulations, and fine-tune as necessary moving forward.

"My company is not regulated."

Some industries are heavily regulated, such as financial services and healthcare, and are required by regulations and laws

such as SEC 17a-4 and the Health Insurance Portability and Accountability Act (HIPAA). Organizations whose business communications are not under such intense scrutiny often believe they don't need to preserve email records. Wrong. Electronic discovery applies to all organizations that could be litigated against. Unlike industry-specific regulatory requirements, the FRCP has a very broad scope. Any company, public or private, that is subject to litigation will be affected. 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.

Recommendations

In the short term, it's better to have a broad policy for archiving in place and implement an archiving software product immediately, then fine-tune the policy based on particulars as they are understood. This enables you to efficiently and effectively preserve electronically stored information in the event of litigation and reduces the risk of spoliation. Implementing a broad policy today will help ensure your organization is able to retrieve and produce specific email records in the event of litigation, avoiding costly fines for not being able to do so. You will know what you have and where it's located—one centralized, tamper-proof repository instead of volumes of backup tapes. Therefore, email archiving software is extremely cost effective, both in terms of reducing management time and costs and helping a company better prepare to respond to an e-discovery request or internal investigation. ■

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information-driven world. Headquartered in Cupertino, CA, Symantec has operations in more than 40 countries. For white papers, resources and demos visit: www.enterprisevault.com