

Protecting Your Business in a Changing Regulatory Climate



an Osterman Research white paper
sponsored by:



Contents

Why You Should Read This Report	2
Overview	3
Current Problems with Messaging Management	4
The Status of Archiving	9
Technology Practices and Preferences	11
The KVS/EMC Solution	11
Summary	17
Appendix	19

Why You Should Read This Report

There are three critical problems that an organization faces if it does not adequately manage the data in its messaging systems through the application of an appropriate archiving system:

- **An inability to comply with regulatory requirements.** Although financial services, government and healthcare-related organizations face the most stringent requirements for regulatory compliance, all firms are required to maintain records for periods of sometimes up to 30 years, which includes records stored within a messaging system.
- **Increased legal exposure.** At some point, most firms will be involved in a legal action of some kind. A technical inability to produce court-ordered emails and other electronic documents because of a lack of appropriate email retention practices is no longer considered an acceptable legal defense for not providing these documents during discovery or other phases of a legal action.
- **A loss of corporate knowledge.** The information contained within the typical corporate messaging system represents a large proportion of the knowledge base of the organization. An inability to effectively store and retrieve this information for later use squanders a great deal of the value that the organization has paid employees and others to produce.

There are three critical problems that an organization faces if it does not adequately manage the data in its messaging systems.

This report is important reading for anyone involved in managing a business or a messaging system: first, it presents the current state of the messaging management problem by discussing the results of a survey recently undertaken by Osterman Research. This survey focused on the specific pain points felt by organizations because of inadequate messaging management practices, and the consequences of this poor management. Second, it discusses a new offering from KVS and EMC that provides a cost effective solution to the messaging management and compliance problem.

In short, this document presents the current state of the messaging management problem and what an organization can do to solve it.

Overview

There are a number of messaging-related challenges facing the enterprise today, including:

- Rapid growth in the size of the various message stores in use throughout the enterprise.
- Increasing costs of storage caused by the rapid increase in messaging-related data entering the enterprise.
- Difficulties in archiving all of the data that the enterprise must retain on a long term basis in order to meet regulatory and other requirements.

There are a number of messaging-related challenges facing the enterprise today.

The financial services industry faces the most stringent requirements for compliance because of requirements imposed by the Securities and Exchange Commission (SEC) most notably, but also by the National Association of Securities Dealers (NASD) and other entities. Specifically, broker-dealers are required to comply with a number of requirements, including SEC Rule 17a-4(b)(4), which requires broker-dealers to maintain the original versions of all communications sent and received that relate to their business activities.

Unfortunately for broker-dealers, the SEC has not specified the content that needs to be retained and what can be discarded, but the agency has created a number of very specific guidelines regarding how electronic documents are to be stored. These requirements include the deployment of systems that make it impossible to erase documents during the required retention period, and the ability to verify the integrity of the storage process, among many other requirements.

To understand the depth of the problems faced by financial services and other organizations trying to properly manage their messaging infrastructures, Osterman Research undertook an in-depth research study that was sponsored by KVS and EMC. The purpose of the study was to:

- Understand the current state of archiving in the context of enterprise messaging.

- Understand the problems that organizations face in managing the increasing flood of messaging and related data that enters their organizations.
- Understand how organizations deal with this information and how various government and other regulations impact them.
- Understand how the application of archiving technologies could solve the current problems faced by messaging administrators.

In order to accomplish the goals of this project, Osterman Research surveyed 100 organizations in North America that serve a variety of industries, including manufacturing, government, utilities and life sciences. These organizations range in size from 500 to 150,000 email users, with a mean of 12,500 users per organization. The surveys were conducted with members of the Osterman Research survey panel using Web-based surveys during the period March 10 through March 27, 2003.

Current Problems with Messaging Management

During the previous 12 months, the average message store size has increased by 40%.

The total amount of information housed in the typical message store is increasing dramatically: our research demonstrated that during the previous 12 months, the average message store size has increased by 40%, although many organizations have experienced growth of 100% or more during this period.

The primary contributors to this growth have been increasing use of attachments (cited by 68% of respondents as a major contributor to the increase in message store growth), the increasing use of email in general (64%) and spam (43%). In fact, Osterman Research believes that the degree to which spam is contributing to the overall growth in message store size may actually be underestimated: spam currently accounts for about 70% of all email traffic at present, and a significant percentage of organizations do not yet have in place adequate spam filters. This results in an enormous amount of unwanted email reaching end users, filling backups and archives, and so forth.

Other contributors to the increasing growth in the size of the message store include two factors that are directly relevant

to the archiving issue: increased legal concerns about data retention, cited by 27% of respondents as a major contributor; and increased regulatory requirements (16%).

In 45% of organizations, there is no mechanism in place to ensure that users do not delete messaging system content that is important for the organization to retain on a long-term basis.

There is an Enormous Potential for Data Loss

Our research has found that about 60% of the critical data that a typical email user needs to do his or her job is housed in the messaging system, either as attachments, messages, contacts or other information. Consequently, because this information is valuable to users, it is valuable to the organization that employs these users, since the organization has paid them to create and make use of this information on a regular basis. Further, our research found that 54% of organizations believe that access to their organization's messaging system and content in the context of business continuity and disaster recovery is "extremely important", while another 27% believe it to be nearly as important.

However, our research indicates that in 45% of organizations, there is no mechanism in place to ensure that users do not delete messaging system content that is important for the organization to retain on a long-term basis. In another 10% of organizations, individual users are responsible to ensure that this data is retained long term. In other words, in more than one-half of organizations, there is no automatic mechanism in place to make sure that users don't delete critical data that must be kept long term. In response to the question about ensuring that users do not delete critical messaging system content that must be kept long term, one messaging administrator at a large financial institution told us, "We hope, and sometimes we go to church on Sunday to pray, they do not."

In response to the question about ensuring that users do not delete critical messaging system content that must be kept long term, one messaging administrator at a large financial institution told us, "We hope, and sometimes we go to church on Sunday to pray, they do not."

The problems caused by a lack of proper messaging management range from bad to worse: in an unregulated company, poor messaging management can make a company less efficient and could potentially create regulatory or legal problems; however, the lack of proper management in a regulated company – such as a stock brokerage – can result in significant financial penalties. For example, in December 2002, five Wall Street brokerages were fined a total of \$8.25 million by the SEC because they did not retain certain emails for the required retention periods and because they did not comply with other SEC requirements in a timely manner.

In 78% of organizations, users store information in local message stores, but in only 46% of organizations are local message stores included in regular backup... this means that an enormous amount of information is simply bypassed by normal IT backup procedures..

In the event of a regulatory requirement to produce all data on a given topic, organizations with such a loose data retention practice would be very hard pressed to meet this requirement and so could be subject to significant penalties.

Local Message Stores Make Information Unavailable

Our research found that in 78% of organizations, users store information in local message stores, but in only 46% of organizations are these local message stores included in the regular backups of the messaging system. Further, the median size of each local message store is 175 megabytes. What this means is that an enormous amount of information is simply bypassed by normal IT backup procedures. This has two important implications:

- First, there is an enormous amount of information that is simply unavailable to the organization as a whole when locally stored messaging information is not included in the corporate backup. For example, in an organization of 2,500 users in which only 50% of users have local message stores that are not backed up, there is 214 gigabytes of information that is unaccounted for outside of the corporate backup – if we assume that a typical message is 50 kilobytes, then nearly 4.5 million messages are left in local message stores at any given time.
- Second, because this information is not included as part of the corporate backup and is not readily available or searchable by the IT department, much of the corporate knowledge that this mass of information contains is simply lost because it is not available to all users. Worse, in the event of a regulatory requirement to produce all data on a given topic, organizations with such a loose data retention practice would be very hard pressed to meet this requirement and so could be subject to significant penalties.

Mailbox Quotas Restrain Employee Productivity

Mailbox quotas are useful because they limit the amount of storage that must be maintained online, thereby improving the performance of these servers and minimizing the amount of time required to restore a messaging server in the event of a crash. Most organizations impose quotas on the maximum size of the personal message store available to users: our research found that 65% of organizations impose such quotas, and that the average size of a mailbox quota is 116 megabytes.

The problem with quotas, however, is that they impose limits on what users can do with their messaging system, and they require users to spend time deleting old emails in order to stay under the quota. Further, our research found that 28%

of users complain to some extent about the size of their quotas.

This can create two problems for an organization: first, if users must spend time managing their own mailboxes in order to stay under the quota, they are simply less productive, since they are performing a task that could easily be automated by an appropriate archiving system. Second, users may be tempted to simply delete old emails if faced with a quota-imposed inability to send or receive a critical email. This can result in an enormous liability to an organization, particularly a regulated one. In short, the active enforcement of quotas, which often leaves policy enforcement in the hands of employees, can result in the loss of critical business information.

Only 57% of the organizations surveyed have an email retention policy in place.

Many Organizations Lack Email Retention Policies

Only 57% of the organizations we surveyed have an email retention policy in place. Worse, in only 22% of the organizations that have an email retention policy does the policy differentiate between different types of email. Among those organizations that do have an email retention policy, there are a variety of entities within the organization that determine email retention policies, including the legal department, the IT director/manager and the CIO.

Explaining the relatively low percentage of email retention policies that are currently in place may be the fact that only 29% of organizations surveyed *believe* that they have a legal or regulatory requirement to retain email for a minimum period. However, among the organizations that we surveyed that do have a legal or regulatory requirement to retain email for a minimum period, 61% of the organizations are in the financial services industry, 21% are in the government sector, and 7% are life-sciences related firms. These are the industry sectors that face the most stringent requirements for email and other data retention requirements.

Our research also found that 72% of organizations have no requirement to maintain copies of email separately from the operational email system, although 13% of organizations do have such a requirement for all email, while another 4% have such a requirement only for external email.

Backup and/or Archiving Requirements Will Increase

Just over 50% of organizations have not experienced any significant change in their backup and/or archiving

requirements during the past 12 months. However, during the next 12 months, the majority of organizations believe that their requirements in these areas will become more stringent. Among the areas in which these requirements are anticipated to become more difficult are more stringent regulatory requirements, corporate retention policies being put in place where they do not exist today, the requirement for longer retention periods, and the requirement to implement faster and larger capacity storage systems to handle the growth of email.

Many are Not Satisfying Regulatory Requirements

Our research found that if an individual email in the messaging system had to be restored, the oldest email that could be restored would be an average of 298 days, or about 10 months old. This is a significant problem in that many regulatory requirements, not just those that impact the financial services industry, require that records-based information in emails be kept for much longer periods. For example, while SEC and NASD requirements dictate that emails are kept for a period of six years or more, some Occupational Safety and Health Administration requirements require that records be kept for 30 years.

Our research also found that to restore the oldest email currently retrievable, it would require an average of 9.6 person-hours for an IT staff member to complete the recovery, or 1.2 days of staff time simply to recover a single email.

We also found that during a typical month, there are 4.6 requests per 1,000 email users to retrieve an individual email or group of emails from the backup or archive in response to litigation, a human resources dispute or simply to respond to a user request for one or more old emails. Further, the IT department has the time to fulfill, on average, only about 73% of these requests – 22% of IT departments have the time to fulfill only one-quarter or fewer of these requests.

If we conservatively assume that the typical request to retrieve an individual email requires an average of three hours to complete (less than one-third the amount of time required to retrieve the oldest email), an organization of 10,000 users would require 0.8 full-time equivalent staff members simply to recover old emails. At a fully-burdened annual salary of \$75,000 for this staff position, the cost to the organization would be \$60,000 per year simply for the labor required to recover old emails. While this represents an

To restore the oldest email currently retrievable, it would require an average of 9.6 person-hours for an IT staff member to complete the recovery, or 1.2 days of staff time simply to recover a single email.

During the past three years, 72% of organizations have been required to search through backup tapes for old emails. An organization that relies solely on backup tapes as the underpinning of its compliance strategy is taking a tremendous risk.

Most IT departments have been required – or will be required – to search through backup tapes to retrieve one or more old emails in response to such a request. Our research found that during the past three years, 72% of organizations have been required to conduct such a search.

expense that would be eliminated through the use of appropriate archiving technology, it also represents the application of skilled and scarce IT staff resources to a task that could easily be automated and require no IT involvement.

Exacerbating the data recovery problem is that most IT departments have been required – or will be required – to search through backup tapes to retrieve one or more old emails in response to such a request. Our research found that during the past three years, 72% of organizations have been required to conduct such a search. If this request comes from a regulatory agency with the authority to impose significant fines on an organization for non-compliance, an organization that relies solely on backup tapes as the underpinning of its compliance strategy is taking a tremendous financial risk, not to mention potential damage to its reputation.

The Status of Archiving

The deployment of archiving systems is not keeping up with the need for it. Despite the increasing requirements to archive messaging data for varying periods and, as demonstrated in the previous section, the problems with not doing so, our research demonstrates that the vast majority of organizations do not yet have in place an adequate archiving system that will provide long-term retention of data and that will maintain the integrity of this data. Most organizations continue to keep data on backup tapes, and only about one-half of organizations actually keep critical data long term, either on tape or in an archiving system.

The vast majority of organizations do not yet have in place an adequate archiving system that will provide long-term retention of data.

Interestingly, despite the fact that only 16% of organizations actually have deployed a messaging archiving system, 66% of respondents indicated that such a system would be either “desirable” or “very desirable”. In contrast, only 33% of respondents indicated that a tape backup system in which data is kept only for a maximum of 90 days would be desirable or very desirable, despite the fact that nearly 50% of organizations employ this strategy for backing up their messaging system.

Current Practices are Not Proactive

As further evidence of the current lack in corporate archiving policies, we asked organizations about the extent

to which their messaging archiving policies were “proactive” with regard to maintaining compliance with all applicable legal and other requirements for their respective industries. What we found was somewhat surprising: only 8% of organizations believe their organization’s messaging archiving policy is “very proactive”, while 24% believe that it is “very reactive”. Even more interesting is the fact that 31% of organizations believe their organization’s messaging archiving policy should be very proactive. On the bright side, however, 19% of organizations believe that their messaging archiving policies will be very proactive within 12 months, a significant increase above current levels, although dramatically below what should be the case given the well-publicized accounts of problems faced by companies that were not sufficiently proactive in managing their messaging system content.

A significant percentage of organizations believe that handling messaging system storage growth cost effectively over the long term will be relatively difficult.

Handling Messaging System Storage Growth Will Be Difficult

A significant percentage of organizations believe that handling messaging system storage growth cost effectively over the long term will be relatively difficult: our research demonstrates that 8% of organizations believe that handling such growth cost effectively will be “extremely difficult”, while another 22% believe it will be nearly as difficult.

Archiving Will be the Key to Managing Email Growth

An alternative to archiving in a messaging system (albeit not an adequate one) is simply to add more storage to the system in order to handle the growing quantity of email traffic experienced by most organizations. When we asked organizations to rate the adequacy of storage solutions vs. archiving as a means of managing email growth, we found that 21% of organizations believe that archiving is a critical component in managing this growth, while only 7% believe that storage solutions alone are sufficient to manage this growth.

In 12 months, 32% of organizations believe that archiving will be a critical component in managing email growth.

Although most organizations are currently leaning toward archiving as a better solution to handle email growth than storage solutions alone, the trend is definitely moving more toward archiving as a better solution to handle email growth. When asked how they would answer the question posed above in 12 months, 32% of organizations believe that archiving will be a critical component in managing email growth, while only 6% believe that storage solutions alone will be adequate.

Technology Practices and Preferences

Currently, most organizations employ server-based storage in their email infrastructure. A minority of organizations currently support either storage-area networks (SANs) or network-attached storage (NAS).

Our research also focused on the types of storage that organizations would prefer for messaging system content based on its age. We found that for messaging system content up to one year in age, optical is the preferred storage medium, followed by tape and then magnetic storage. This is due primarily to optical's write-once nature, which preserves the integrity of data written to the medium; and the perceived temporary nature of magnetic storage.

Our research also determined that 38% of organizations have a requirement of some sort to save historical email on non-erasable media, such as optical.

For messaging system content that is more than one year old, optical media has an even greater desirability.

Thirty-eight percent of organizations have a requirement of some sort to save historical email on non-erasable media, such as optical.

The KVS/EMC Solution

Because this research program was sponsored by KVS and EMC, we asked several questions about the desirability of key attributes of an archiving solution that has been developed by both companies and that is discussed later in this document. However, we did not identify the vendors in order to eliminate any potential for bias in the research.

The solution that we presented to survey respondents for consideration was introduced with the following information, after which several questions were posed:

Imagine that your organization had implemented an archiving system for your messaging infrastructure that automatically removed older messages from users' mailboxes, archived them and provided full text-searching capabilities for the archived content. Because the archiving system would place shortcuts to the archived content in each mailbox, users would still have access to this old information without any administrator involvement, just as if the information was stored in their individual mailboxes.

Other features of such a system would include:

- *The ability to automatically match the type of storage to the age of the archived content in order to reduce storage costs.*
- *Protection of archived information so that it cannot be modified in compliance with regulatory requirements. Archived emails and other messaging system information are preserved in their original format.*
- *Single-instance storage which can significantly reduce the amount of total storage capacity required in the archive.*

Respondents to the survey indicated that the [KVS/EMC] system would provide a number of advantages to their messaging system management.

Respondents to the survey indicated that the system described above would provide a number of advantages to their messaging system management, including reduced involvement from IT in managing the system, reduced costs, faster retrieval of messaging information, reductions in storage capacity requirements and ease of use, among other advantages.

Our research also indicated that the potential market for this solution tends to favor a solution that would archive messaging system content, as well as content from other information sources.

Key Requirements

Any archiving system that is employed to support the long-term compliance requirements of the enterprise AND to make users of messaging and other systems more productive must possess a number of attributes, including:

- The ability to maintain the long-term integrity of the archived data, preventing it from being altered over time.
- The ability for the data to be readable for several decades.
- The rapid and complete retrieval of all relevant information to support any and all compliance requirements that the enterprise might face.
- The ability to meet all regulatory, legal and other requirements now and in the future.

The potential market for [the KVS/EMC] solution tends to favor a solution that would archive messaging system data, as well as data from other information sources.

- Applicability for use across the entire enterprise.

**KVS Enterprise Vault/EMC Centera Compliance Edition:
The Marriage of Leading Edge Compliance Technologies**

KVS, in conjunction with EMC, has developed an integrated software and hardware archival storage solution that is specifically designed to address the challenges of those responsible for managing content in regulated industries.

- KVS Enterprise Vault is a leading content archiving solution for Microsoft Exchange environments. From a user perspective, Enterprise Vault operates seamlessly: each archived email is replaced with a shortcut in users' mailboxes, each of which links to the original email and attachment that is housed within the archive. Because content is archived automatically, even users with mailbox size quotas can use their messaging system as if their mailbox size was limitless.
- EMC Centera™ Compliance Edition is a purpose-built, magnetic-disk-based records storage solution designed to overcome the limitations of conventional archiving technology, while enabling an enterprise to comply with the most stringent records standards and regulations.

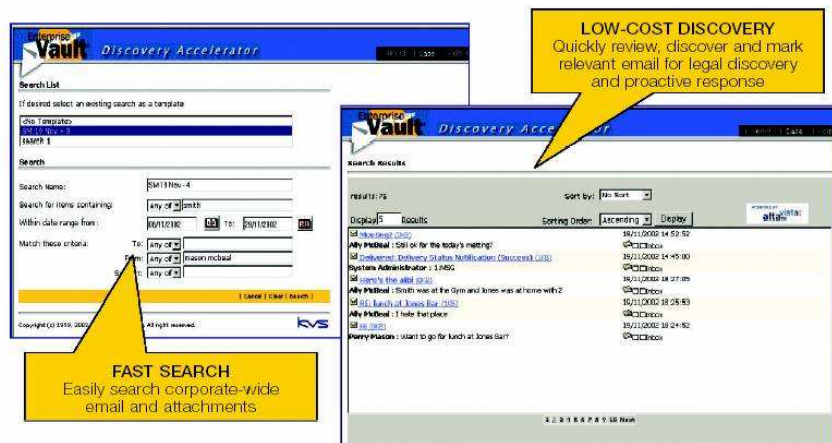
This combination enables organizations to comply with the myriad, and increasingly stringent, set of email retention requirements imposed by the SEC, NASD and other entities.

The key to Centera is "Content Addressing" – a digital fingerprint that is derived from the content itself.

As part of this offering, KVS provides its Compliance Accelerator, which specifically addresses the requirements of NASD 3010 and NYSE Rule 342 (these rules focus on the active, supervisory review of employees' communications, including email.) Compliance Accelerator makes the necessary process of compliance review and enforcement much more efficient, because it allows the creation of structured review processes, it tracks these processes, and it allows an organization to demonstrate that it is in compliance with its policies.

Complementing Compliance Accelerator is Enterprise Vault Discovery Accelerator. Discovery Accelerator allows authorized reviewers, such as corporate litigation staff, to quickly target and pinpoint specific email messages when they are needed as part of litigation support, legal discovery or investigation. With no IT dependencies for locating email from backup, Discovery Accelerator provides a high level of organization and structure to an email system and enables

content to be quickly tracked, reviewed and marked for either lead counsel examination or court-ready production. This greatly reduces the cost of electronic discovery because relevant email can be easily searched, qualified and rapidly brought to the surface. The support of global marking schemes also means that an organization can avoid unnecessary duplication of review effort when discoveries overlap. Shown below is a screen shot of the Discovery Accelerator interface.

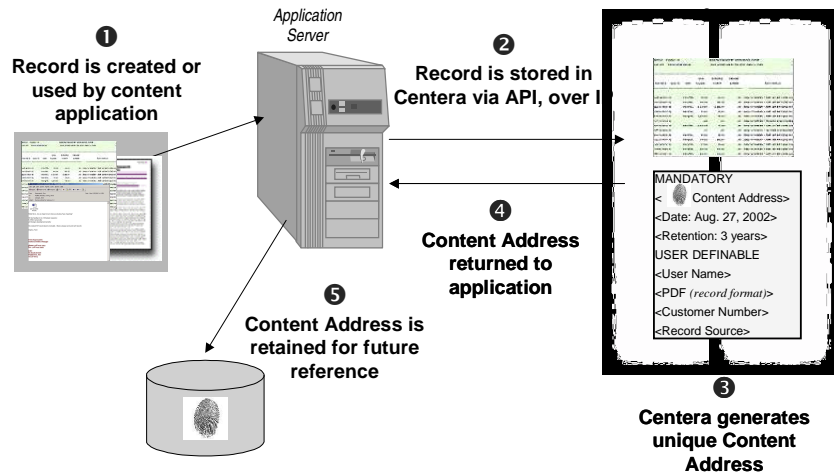


The impact of litigation and regulation on business activities may require proactive, or at least reactive, investigation of email content. The KVS Compliance and Discovery Accelerators are designed to deliver the most appropriate solution to meet specific business requirements for reviewing email content. Enterprise Vault, used in conjunction with these Accelerators, has been designed to deliver reliable and timely access to email-based records.

Content Addressing Acts as a Digital "Fingerprint"

The key to Centera Compliance Edition is "Content Addressing". Each record stored in Centera is assigned a unique Content Address, a sort of digital "fingerprint" that is derived from the content itself. Any change to a record housed in the archive will result in the creation of a new Content Address for that record. In conjunction with the creation of the record, Centera also stores and manages a Content Descriptor File, which includes data about the record, including creation date, its format, the period for which the data must be retained, and any additional user-defined business logic. The content address for the Content Descriptor File is then returned to the application and used as the handle for any future retrieval requests.

The following diagram provides an overview of how Centera Compliance Edition works.



Compliance Edition provides the ability to associate and enforce multiple retention periods with each electronic record.

Centera Compliance Edition fits seamlessly into an existing IT infrastructure. With Centera Compliance Edition, similar to existing records storage systems, users create and manage electronic records with a variety of software applications, including email archiving systems, document management systems, imaging systems, backup systems and other systems. However, unlike traditional storage systems, Centera Compliance Edition brings a set of unique innovations to simultaneously enable compliance, eliminate risk, and reduce costs.

Retention Periods Are Enforced

Centera Compliance Edition also provides the ability to associate and enforce retention periods with each electronic record. Once a retention period is set for a particular record, the system will lock the record and guarantee that it cannot be deleted until the retention period expires. Multiple retention periods can be associated with a single record, so if it is subject to multiple regulations, or if a retention period must be extended because a record is subject to a legal hold, the system will protect it until the longest retention period has expired. Further, retention periods can be defined within Enterprise Vault and then enforced by Centera.

By enforcing retention at the record-level, Centera Compliance Edition eliminates the exposure, risk and cost of managing retention of a handful of records by saving entire optical platters or tape cartridges. With Centera, this

protection is enforced at the storage subsystem level so that it is inaccessible to eternal interference and cannot be overridden by user error or malicious actions. Centera does not proactively delete records once their retention period has expired, but instead simply unlocks the record at the time of expiration so that users can leverage their integrated software applications to implement a defined record disposition strategy.

Compliance Edition was architected around the most stringent storage media standards that exist in the world today.

Centera Compliance Edition was architected around the most stringent storage media standards that exist in the world today. Centera's Content Addressing ensure that each record cannot be overwritten, while retention protection makes certain that a record cannot be prematurely erased before the expiration of its retention period. Unlike any other media, Centera can ensure the integrity of the records throughout its lifecycle through an automated system of continuous data integrity checking as well as onsite and offsite protection mechanisms. Centera provides the integrity of WORM media with the cost efficiency and speed of access provided by magnetic storage.

Long-Term Compliance

Perhaps the single most pressing challenge associated with storing records that are subject to regulatory review is ensuring access to those records several decades after their creation when storage technologies change and some vendors are either no longer supporting legacy technologies, or are no longer in business. Centera's ability to ensure access to content over many years is facilitated through the Content Addressing architecture and the related Application Programming Interface (API). Centera provides a future-proof architecture that can be migrated across generations of Centera technology. These capabilities combine to provide a robust solution for the challenges of long-term retention of records.

Additional Benefits

Other benefits provided by Centera Compliance Edition include:

- **True integrity of replicated content.** Centera Compliance Edition guarantees archiving transaction integrity, even across replicated sets. When content is replicated from a source to a replica content set, the content will not be regarded as fully archived until the replica has confirmed that it has received the content.
- **Greater throughput.** The use of connection pooling enables greater throughput, particularly over wide-area network connections and through firewalls. This feature is particularly important for large, geographically distributed organizations – the norm among the largest financial services providers.
- **More efficient storage and better performance.** Where email attachments already exist in a Centera-based archive, a new email that enters the archive, but that references the previously archived attachment, will share the attachment with the older email, thereby reducing storage requirements and improving system performance.

Regulatory, legal and other requirements have become more numerous and more stringent, dramatically increasing the exposure of enterprises to a growing variety of legal and other liabilities, and increasing the severity of the consequences for improper archival of critical business data.

Summary

Messaging systems have become the de facto information store for a wide variety of critical business data, resulting in dramatic increases in the total quantity of information stored in these systems year after year. At the same time, regulatory, legal and other requirements have become more numerous and more stringent, dramatically increasing the exposure of enterprises to a growing variety of legal and other liabilities, and increasing the severity of the consequences for improper archival of critical business data.

However, most enterprises have not adequately addressed the problems that they face from growing message stores and increased legal liabilities. For example, most enterprises continue to allow individual users to maintain information in local message stores outside the bounds of a centralized data repository, nearly one-half of enterprises have not established an email retention policy, and only one in six

enterprises has implemented an archiving system that will permit reliable access to data over long periods.

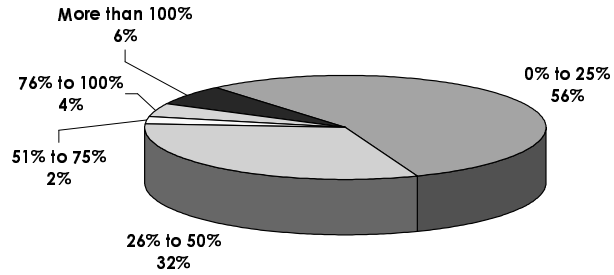
What enterprises require is a means of archiving data reliably so that its integrity is preserved for decades, if necessary; and a means of retrieving this data efficiently and completely in order to meet any and all regulatory, legal and other requirements.

KVS and EMC have joined forces to develop a solution that enables enterprises to address each of these requirements. Their solution integrates easily into the existing IT infrastructure and allows an enterprise to meet all of its regulatory and other requirements for data archival, effectively eliminating the risks and liabilities that most enterprises today face from improper archival practices.

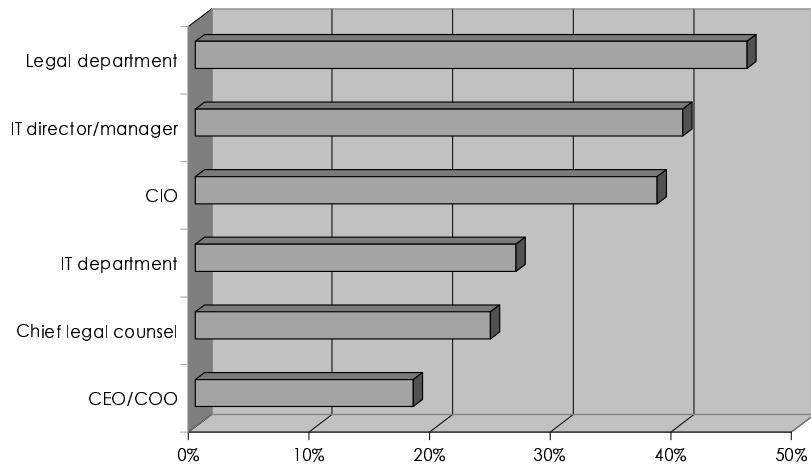
Appendix

The following charts summarize the data developed during the research program conducted for this white paper.

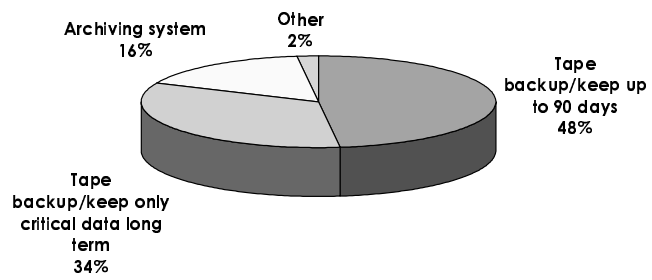
Percentage Growth in Total Message Store Size During the Previous 12 Months



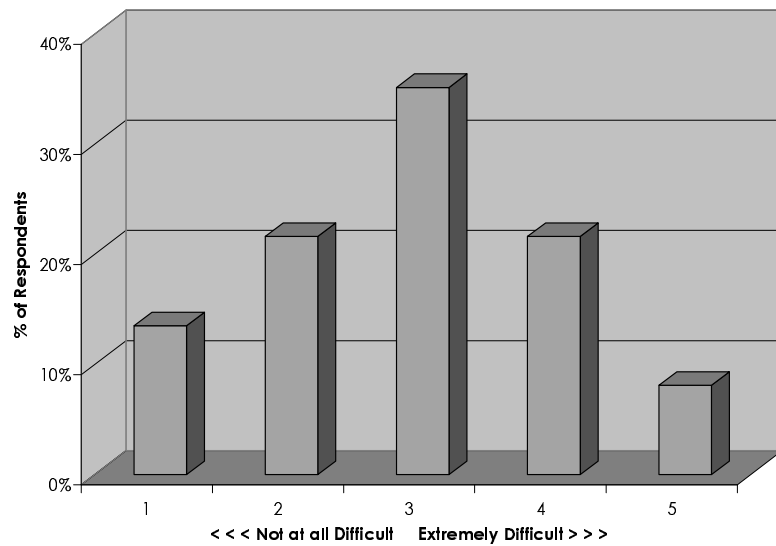
Individuals and/or Groups that Determine Email Retention Policies



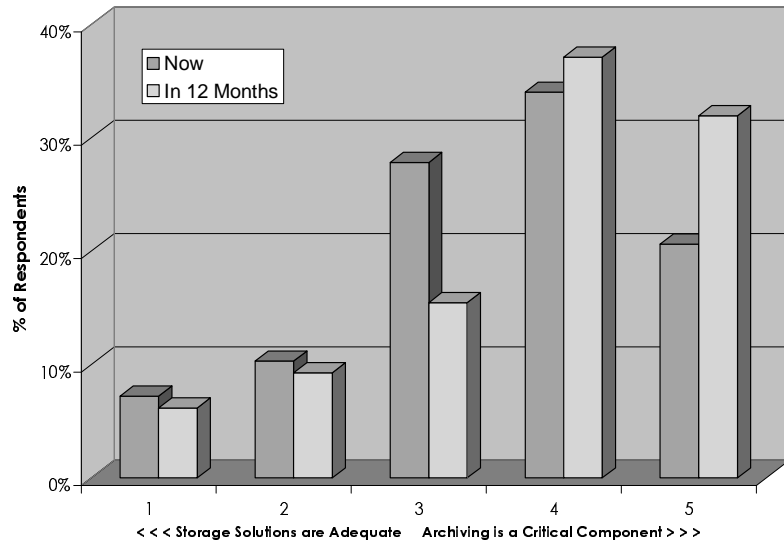
Messaging System Backup and/or Archiving Strategies



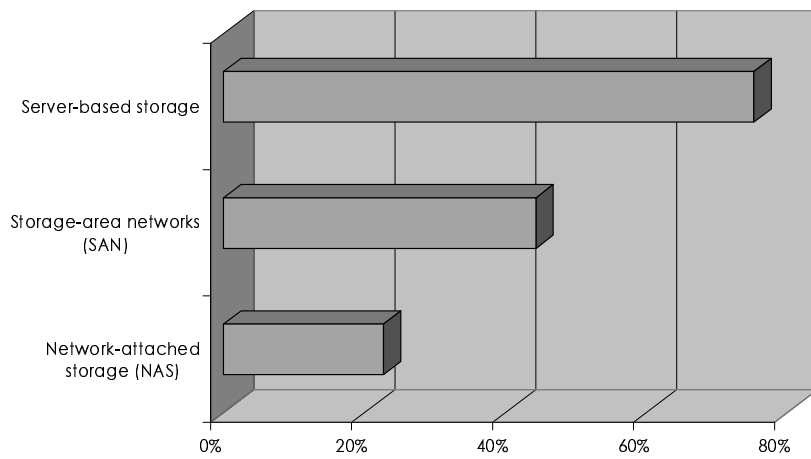
Attitudes Toward Handling Messaging System Storage Growth Cost Effectively Over the Long Term



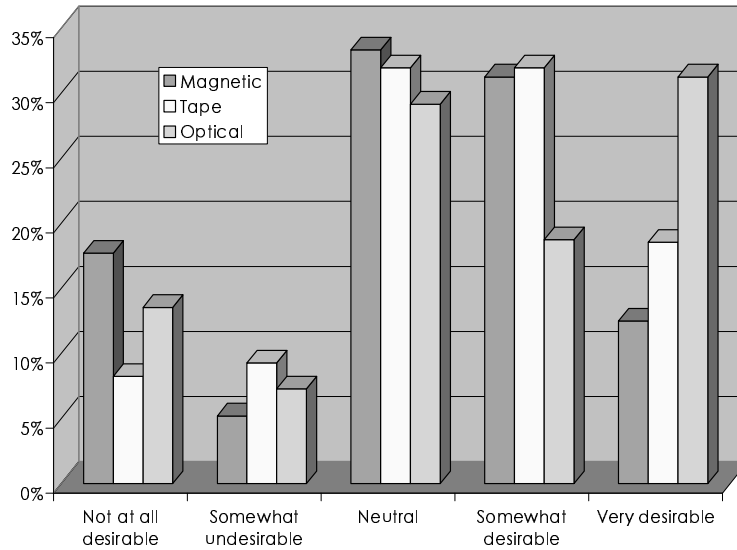
Current and Future Attitudes Toward the Adequacy of Storage vs. Archiving in Managing Email Growth



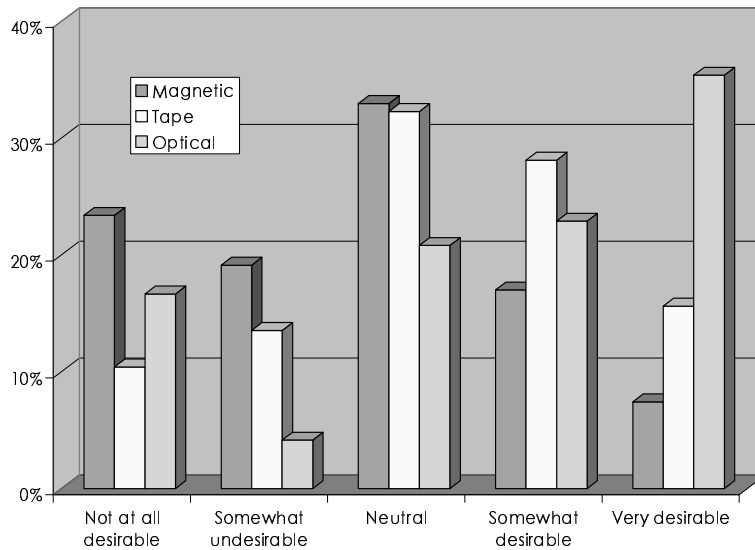
Types of Online Storage Used for Email



Desirability of Various Media for Storing Messaging System Content that is Up to One Year Old

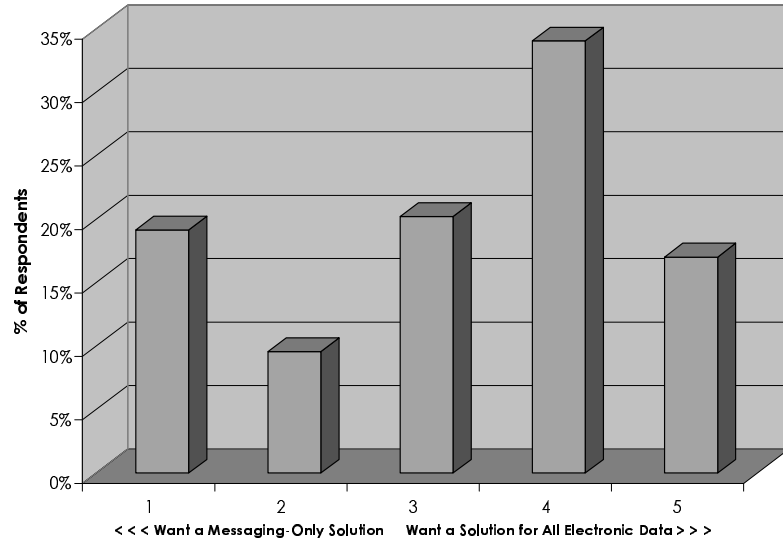


Desirability of Various Media for Storing Messaging System Content that is More Than One Year Old



The Growing Need for Archiving in the Enterprise

Preferences for a Messaging-Only Solution vs. One that Archives All Electronic Data



© 2003 Osterman Research, Inc., KVS and EMC Corporation
All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed outside of the client organization that has purchased it, nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.