



Sunbelt  
**Exchange Archiver™**

SUNBELT EXCHANGE ARCHIVER FOR MS-EXCHANGE ENVIRONMENTS



*Key Issues in Messaging Archiving*



Sunbelt Software

## Key Issues in Messaging Archiving



Sunbelt Software

<b>How Do Organizations Archive Messages? .....</b>	<b>2</b>
<b>What is the Messaging Problem? .....</b>	<b>2</b>
<b>The Top 10 Problems Reported by Organizations .....</b>	<b>4</b>
<b>Where Can Archiving Help? .....</b>	<b>4</b>
<b>What is the Importance of Archiving? .....</b>	<b>5</b>
Regulatory Compliance .....	5
Electronic Discovery .....	6
Storage Management .....	6
Knowledge Management .....	7
Disaster Recovery .....	7
Business Continuity .....	7
Support for Traveling Employees .....	7
Self-Service for Employees .....	7
Preserving the Context of Communications .....	7
<b>The Consequences of Failing to Archive .....</b>	<b>8</b>
<b>The Consequences of Storing E-Mail Exclusively on Backup Tapes .....</b>	<b>8</b>
<b>Backups Versus Archiving .....</b>	<b>9</b>
<b>The State of Archiving .....</b>	<b>9</b>
<b>Recommendations .....</b>	<b>10</b>
Understand the Organization's Requirements .....	10
Establish an Archiving Policy .....	10
Archive .....	10
<b>Consider the Risks of Failing to Archive .....</b>	<b>10</b>
<b>About Sunbelt Exchange Archiver .....</b>	<b>10</b>

This document describes key issues in the archiving industry, including some of the reasons for archiving messages and some of the drivers in the industry.

Osterman Research is a market research and consulting firm that is focused heavily on studying the role of electronic communications in the workplace. This includes e-mail, instant messaging (IM), voice over IP (VoIP), collaboration, and Web 2.0, as well as all of the related technologies and drivers, including security, archiving, and encryption. Osterman Research conducts a lot of primary research, mostly among IT professionals and end users. This research is conducted in order to learn about the problems they are experiencing, what motivates the decisions they make, the prices they want to pay for products, their plans for the near future, and so on.

Focusing heavily on the primary research aspect makes it possible to understand the problems that people are experiencing and how they try to solve those problems. Osterman Research's focus is on electronic communication in the workplace.

## How Do Organizations Archive Messages?

The goal of this document is to describe archiving—meaning, the preservation of business records—and the reasons for doing so. For example, most people file a tax return every year, make a copy of that tax return, put it in a file cabinet, and keep it for seven years per IRS recommendations. After filing a tax return, most people do not pull it out of the file cabinet after 30 to 90 days and run it through a shredder.

However, this is what most people in business do with their e-mail records, instant messaging conversations, and other contacts, as illustrated in Figure 1.



Figure 1

Organizations tend to store these kinds of records on a backup tape for 30, 60, or 90 days. They will keep these records on a hard disk for a short period of time and then throw those records away. This is not a best business practice, but it is what most organizations do today.

## What is the Messaging Problem?

Messaging is a very useful tool, but it is also a serious problem for most organizations. Clearly, e-mail is the most important business tool in use today. A survey of end users asked what percentage of the

information sent by an organization (including paper, electronic communication, telephone, and so on) is accounted for by e-mail. Organizations reported that 74% of information is sent through e-mail, making it a critical business tool.

E-mail is the de facto file transport mechanism. Most people do not use FTP for sending files. Instead, they use e-mail, even for sending 5 MB to 10 MB files. E-mail use is growing at a rate of about 20% per year. Message stores are growing from 25% to 35% per year, depending upon the size of the company, the industry, and so on. For many companies, this growth rate is 50% to 100% per year. Therefore, e-mail storage is becoming a very critical issue, primarily because of all the attachments and everything else that is stored in e-mail.

The average employee sends and receives about 140 e-mails every day. This means that 20,000 to 30,000 e-mails per employee per year are sent and received. The average user spends 34% of each day using an e-mail client. This activity includes looking for contacts, looking for old attachments, sending and receiving e-mail, and managing tasks. Therefore, e-mail is critical for almost everybody who uses it.

An e-mail message contains very valuable content. E-mail is not just for simple communication anymore. People use it to send purchase orders, contracts, and customer communications. Message threads and other very important content are stored in e-mail. It has become the primary repository for many types of critical business records. IT professionals report that their number one problem in managing e-mail is growth in e-mail storage. This has been their main problem for about three years. In the surveys that Osterman Research has conducted, IT professionals have chosen from a list of 35 to 45 problems, rating each problem on a scale of one to five. Consistently, growth in e-mail storage is the number one problem, for all the reasons already described.

For example, suppose a company has 3,000 employees. In 2007, they generated 8,000 archivable messages per day. With e-mail use growing 20% per year and the need to store e-mails for seven years on average, this company's employees will generate an archive of 310 million messages in that seven-year period.

By comparison, a company that has 25,000 to 50,000 employees is likely to generate two to four billion messages that have to be stored for the seven-year period. Searching through this much content is extremely difficult without the right tools. One survey found that 49% of people have difficulty finding records, meaning, going back and finding the content they need. In another survey, 94% of people said they referred to an old e-mail when composing new e-mail.

Consider this example: Suppose a new marketing manager joins an organization and needs to know what the previous marketing manager said to key clients. For example, the new marketing manager wants to find out what was promised to these key clients in the past or what the previous manager had said about a particular project. Searching and finding the content needed is very difficult.

According to the American Management Association (AMA), 24% of organizations have experienced having employee e-mails subpoenaed for a variety of reasons, such as wrongful termination suits. Also, 15% of organizations have gone to court because of lawsuits brought on by their employees' e-mail, such as racist jokes, sexually offensive jokes, videos, and other items sent through e-mail.

This is the messaging problem in a nutshell. No matter how overwhelming and destructive an organization's problems may seem, they probably represent the tip of the iceberg, as illustrated in Figure 2, which shows one of the "de-motivators" that can be found at <http://despair.com>.

The "tip of the iceberg" problem is especially true for e-mail. E-mail use is growing 20% per year, and e-discovery is driving the need to preserve communication. There is more regulation surrounding e-mail. Messaging is bound to become a much more serious problem in the future, and it is especially serious if an organization has no way to preserve messages in a meaningful way.

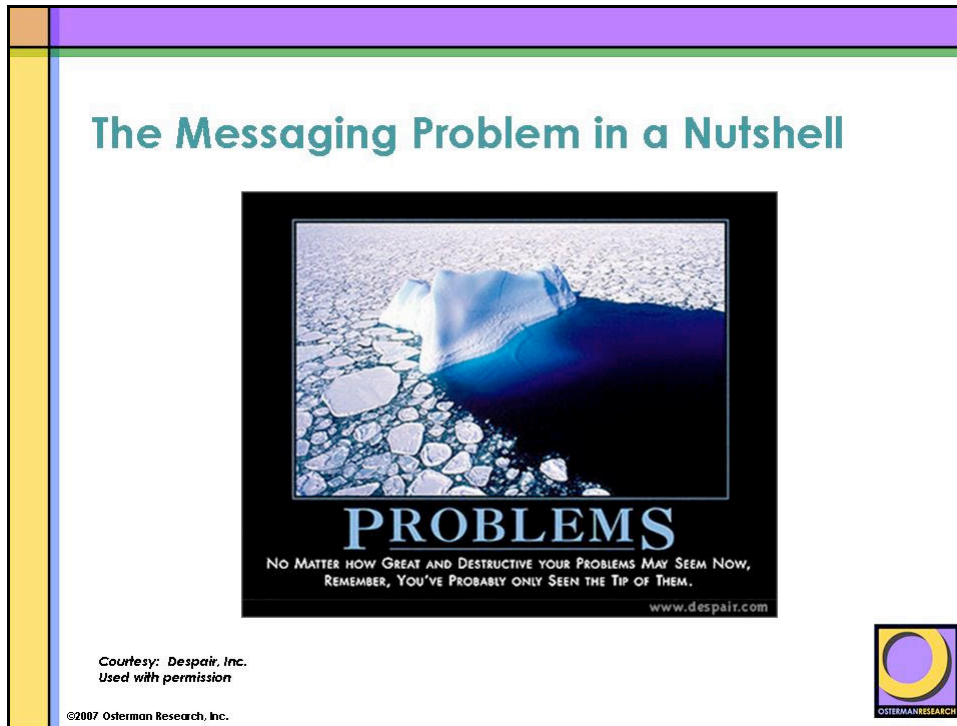


Figure 2

## The Top 10 Problems Reported by Organizations

The top 10 problems reported by organizations are:

1. Growth in e-mail storage requirements (58%)
2. E-mail continuity/disaster recovery (48%)
3. Inadequate e-mail archiving (48%)
4. The amount of spam received (45%)
5. Large attachments sent through e-mail (43%)
6. Employees sending/receiving inappropriate content (37%)
7. Storage of e-mail for compliance (36%)
8. Data loss from employees sending confidential data via e-mail and IM (35%)
9. Employees sending confidential data via e-mail and IM (34%)
10. Users complaining about mailbox quotas (34%)

Growth in e-mail storage is the most important problem. It is reported to be a worse problem than spam, viruses, and spyware because of the sheer volume of content to manage. Also, IT is increasingly called upon to search through that content and is expected to produce it for a variety of reasons. Storage of e-mail for compliance is becoming critical.

## Where Can Archiving Help?

An archiving system can help solve problems in the six areas from the list of top 10 problems reported by organizations:

- Growth in e-mail storage requirements

- E-mail continuity/disaster recovery
- Inadequate e-mail archiving
- Large attachments sent through e-mail
- Storage of e-mail for compliance
- Users complaining about mailbox quotas

An archiving system is not a panacea. It will not solve every problem, but it can provide a major benefit for many problems, such as managing growth and e-mail storage requirements, e-mail continuity in disaster recovery, and making sure that everything stays up and running. An archiving system can be very useful for large attachments sent through e-mails, as well as managing e-mail for compliance purposes (such as e-discovery or regulatory compliance).

One of the leading problems for IT happens when users complain about mailbox quotas. When users request more storage and a larger quota, IT must set that up for individual users. Again, archiving will not help solve every problem, but it will help solve many of the problems that organizations experience.

## What is the Importance of Archiving?

Most of the top 10 problems can be addressed to some extent through the use of a good messaging archiving technology. However, the problem is that most organizations today do not use true archiving systems. Many organizations rely on their backup tapes as their "archive." They mistakenly assume that backup and archiving are the same thing.

About 50% of IT decision makers report having an archiving system. But when asked if they have a system that will automatically index content that comes into the organization, goes out, gets sent internally, and then is put into an archival storage that makes it possible to easily search through content on the backend, only 25% of those same IT decision makers report having such a system.

Although many organizations consider their archive to be nothing more than a stack of backup tapes, this is not archiving. Backups and archives are distinctly different.

Why should organizations archive? What are some good reasons for archiving? What are some of the drivers?

## Regulatory Compliance

The first reason to archive is regulatory compliance. Many statutes focus on the retention of records, including:

- Section 17(a) of the Securities Exchange Act
- National Association of Securities Dealers (NASD) Rule 3010
- FDIC Advisory
- Investment Advisors Act of 1940 (hedge funds)
- The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" (GLBA)
- IDA 29.7 (The Investment Dealers Association of Canada)
- FDA 21 Code of Federal Regulations (CFR), Part 11
- Office of the Comptroller of the Currency (OCC) Advisory
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Financial Modernization Act of 1999
- Medicare Conditions of Participation
- Sarbanes-Oxley Act

- Fair Labor Standards Act
- Americans with Disabilities Act
- Toxic Substances Control Act
- Federal Rules of Civil Procedure (FRCP)

Very few statutes focus on the retention of e-mail per se, but many statutes focus on maintaining good records retention policies. For example, anyone in the financial services industry (including brokers, dealers, hedge fund managers, and investment advisors) needs to preserve communications, instant messages, and e-mail messages. The Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), and the New York Stock Exchange (NYSE), for example, have very specific rules about what must be preserved, how long it should be preserved, the media on which it must be preserved, and so on.

Most organizations do not have such strict requirements. For example, a furniture manufacturer in Chicago is unlikely to have any critical requirements around regulatory compliance. Some industries are heavily regulated (such as financial services) and some are lightly regulated (organizations outside the finance industry). Issues for lightly regulated industries include meeting HIPAA requirements, Medicare compliance, and maintaining employee records. For example, suppose an employee sends an e-mail message to a manager requesting a week off for vacation. The Federal Government has ruled that such a message is a personal record that the organization must keep for at least one year. In this example, it is unlikely that anyone would request seeing the e-mails with vacation requests for the last year, but it is a requirement. Legal Counsel usually advises preserving those records for a minimum of a year.

Few of these regulations specify the form. Often, it is not necessary to preserve e-mail. Instead, the organization could print the e-mail message and put the printout into a file cabinet. But because of the growth of and employees' reliance on e-mail, it makes sense to store it in the same medium for the sake of efficiency.

## Electronic Discovery

The second reason to archive is electronic discovery. This is becoming a much more serious issue, mainly because of new amendments to the FRCP in December 2006. Those new amendments acknowledge what people were doing all along: starting to use e-mail and other types of electronic records more and more in lawsuits. Most court-imposed discovery orders today include e-mail and other electronic content as part of what must be discovered. The FRCP rules were originally established in 1938 and are basically the rules for how people sue each other in simple courts.

The new amendments raise the stakes for electronic records. These amendments state that, within a certain amount of time after a lawsuit is filed, an organization must take an inventory of its electronic content that can be produced for discovery. Organizations need the ability to find out what they can readily produce. Therefore, most organizations today will have to go through some sort of procedure to understand the electronic content they have. Typically, organizations want to begin with e-mail, because that is the primary repository of their records. This is becoming a much more serious issue. Some court cases are starting to interpret the FRCP amendments in terms of what is and is not allowed, and one issue that is becoming very critical is the authenticity of records.

For example, in one case, American Express was sued and lost the case because they could not prove the authenticity of their e-mail records. In several similar cases, a judge has determined a ruling because the e-mail records had no time stamp and the defendant had no proof that they had not tampered with those records. This happened because organizations did not have appropriate archiving technologies. Most organizations of any size are at risk of being sued. Therefore, organizations must preserve records simply because of the FRCP requirements, if for no other reason.

## Storage Management

The third reason to archive is storage management. Again, e-mail stores are growing out of control. The number one problem that managers have is managing e-mail systems. This is why storage management is one of the key drivers for archiving.

Most organizations impose mailbox size quotas. About 60% of mid-sized and large organizations in North America impose such a quota, which is typically about 250 MB. However, because attachments are increasingly used and because e-mail is used more often, employees reach those limits on a more frequent basis, which creates many problems.

The chief problem is that users complain about quotas. When users reach their quota limit, they cannot send or receive e-mail. In many cases, it is necessary to delete content, which might be content that should be preserved as business records. Users spend anywhere from 30 to 60 minutes each week just managing their mailbox. They spend a lot of time just managing household chores because they have a quota. IT has to spend time dealing with quotas, setting up the quotas, making exceptions for certain users, and so on. Quotas are necessary in order to maintain the workability of Exchange servers, but quotas are a problem to manage. If an organization has a good archiving system, one solution is to automatically offload content to the archive and give users what seems to be a mailbox of unlimited size. For example, suppose an organization has the appropriate archiving technology. When the mailbox fills up to 80% of the quota, older content is automatically moved to the archive. This reduces the amount of content in the live mailbox, and users never reach their quotas. This means they save 30 or 60 minutes per week because they do not have to maintain their mailboxes.

### **Knowledge Management**

The fourth reason for archiving is knowledge management, which means preserving the corporate memory. Again, most of the content that users send or receive is tied up in e-mail, whether it is the e-mails themselves or the attachments. If an organization purges e-mail stores after 30, 60, 90, or 120 days— as most organizations do today—this results in losing a lot of corporate memory. This can include statements made to an organization's key clients and statements made about old projects. It simply makes sense to preserve the corporate knowledge that has been generated.

As mentioned previously, users need access to old information, and very often they do not have it. If they cannot find it, they either re-create that information or go without it. In either case, they can spend a lot of time looking for old information. In many cases, they do not find the content they need. Knowledge management is almost never the primary reason that an organization implements an archiving system, but it is an important reason because it is an important benefit of archiving.

### **Disaster Recovery**

Another reason for implementing an archiving system is disaster recovery. Suppose an organization is located in a city struck by a hurricane. In this case, the e-mail servers are out of commission for a while. If that organization has an offsite archive, it will have access to its old e-mail stores.

### **Business Continuity**

Many organizations use an archive as their backup e-mail repository so that their business can stay up and running in case of a disaster, a power outage, or a leaky sprinkler pipe above the server room.

### **Support for Traveling Employees**

A company in the Seattle area uses their archive for the purpose of providing complete e-mail access to traveling employees. When these employees are sitting in front of a client and they need to find out what was said to that client a year ago, they have access to that information through a web interface.

### **Self-Service for Employees**

Many organizations ignore employee requests for restoring deleted e-mails because it is too difficult. Most employees either go without them or store e-mails locally themselves.

### **Preserving the Context of Communications**

Many organizations choose not to archive because they want to delete all the "smoking guns." That is a good idea if an organization has access to all of its old e-mail. But if an organization deletes its own copies of e-mail, that organization has deleted about 10% or 20% of the copies. The people who received

the e-mail still have a copy, which could be stored on a backup tape in another organization's archive. It is important to preserve the context of communications, for example, if it is necessary to present that context during a trial.

If an organization's representative is presented with an e-mail during trial and is the only one in the courtroom that does not have a copy of the e-mail, then that organization is at a serious disadvantage. If the organization at least has the copy when sued or when a regulator requests it—if the organization has the ability to preserve that context and present a case for why something was said in an e-mail—then there is a better chance of winning the lawsuit or the regulatory audit.

## The Consequences of Failing to Archive

What are the consequences of not archiving? Consider the following high-profile cases of companies that did not preserve e-mail appropriately.

On several occasions, Morgan Stanley did not provide e-mails that were requested by regulators and in arbitration proceedings. This is a big mistake for organizations that are governed by the SEC, FINRA, and so on. FINRA found that Morgan Stanley had destroyed many e-mails by overwriting backup tapes and by letting users permanently delete e-mail. In 2006, Morgan Stanley had to pay a \$15 million fine to the SEC for not saving e-mail properly. And then in September 2007, FINRA announced Morgan Stanley would pay \$9.5 million to two sets of customers that made claims against the company and that Morgan Stanley would pay \$3 million for not providing e-mail and supervisory content.

For a multibillion-dollar company, \$15 million is not a heavy fine. For smaller companies, the fines can be smaller but still fairly heavy. In another case, the NYSE fined Wachovia Bank \$2.25 million for not complying with the rules of SEC 17(a)—for not preserving e-mail properly. Wachovia Bank did not retain or review certain e-mail records.

In March 2006, Merrill Lynch paid a \$2.5 million SEC fine for not properly archiving e-mail. In March 2004, Bank of America was fined \$10 million by the SEC for failing to keep e-mail records regarding its recent merger and for taking too long to comply with regulatory requests. In December 2002, the SEC fined Salomon Brothers, Morgan Stanley, Piper Jaffrey & Hopwood, Deutsche Bank, and Goldman Sachs a total of \$8.2 million for failure to comply with Rule 17(a)4.

Most of these big fines were the result of financial services companies failing to preserve e-mail properly, but there have been cases in which nonfinancial services companies have been fined or have lost lawsuits. One problem that can result from not preserving e-mail properly is that a judge can instruct a jury to assume that the organization's inability to produce e-mail when requested is evidence of culpability. In other words, the assumption is made that the organization must have had a good reason for destroying the evidence because the organization may be guilty. Judges have instructed juries to that effect. Therefore, any organization can be at a very serious disadvantage if it does not properly preserve e-mail.

## The Consequences of Storing E-Mail Exclusively on Backup Tapes

What happens if an organization has every copy of every e-mail message ever sent from or received by the company, but all e-mail messages are on backup tapes? The problem is not that the organization does not have the information. The problem is finding and extracting the needed information.

Consider these cases in which producing e-mail from backup tapes has been very expensive:

- In the case of *Linnen v. Robbins*, the cost to process backup tapes was \$1.5 million.
- In 2001, the cost of a White House recovery of 246,000 e-mails from about 4,900 backup tapes cost an estimated \$10 million.
- In the case of *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, the cost of restoring 2.3 million e-mails on 93 backup tapes was estimated at \$6.2 million.

If an organization wants to perform the task of restoring e-mails from backup tapes internally and not include forensic firms (which can be very expensive), it is still necessary to invest IT time to set up a

recovery server, load the content from the backup tapes, index it, perform the search, and then produce the results. This can take weeks. In some cases people searched through 3,000 to 4,000 backup tapes to find the information they needed. If it is necessary to bring in forensics firms, it can cost up to \$35,000 to process one tape. If an organization has 1,000 tapes, it will cost \$3.5 million just to get to the point where it is possible to produce the needed e-mails for inside legal counsel.

This is a very expensive process if an organization's only archive is its backup tapes. Also, backup tapes have a reasonably high failure rate. For example, the estimated annual failure rate (AFR) for older backup tapes is about 11%. Even if an organization has all the information on backup, that organization may not be able to access the information because of physical or logical errors on the tape.

In general, backup tapes are a very good best practice. Organizations should run backups nightly or every other night. They are very useful for short-term, snapshot storage requirements, but they are not acceptable for archiving. Backups make it possible to restore a messaging server if it goes down and to provide short-term access to data. However, backups are not a long-term solution for e-discovery.

## Backups Versus Archiving

What do backups accomplish? They allow the restoration of servers after a crash. They preserve a snapshot of the current state of an e-mail server, meaning the content that exists at a given point in time. But backups do not preserve a true record of all e-mail traffic. For example, suppose a company schedules daily backups at 2:00 a.m. A senior manager sends an e-mail to external counsel at 10:00 a.m., stating the reason why the company fired an employee. The external legal counsel deletes that e-mail at 3:00 p.m. and the senior manager who sent the e-mail deletes it at 4:00 p.m. In this case, that message will never be backed up, because it has been both created and deleted within the company's backup window. According to the law, the company is supposed to preserve the e-mail as a business record, but an automated backup will never preserve content in this situation. It will preserve only the content that exists at the time when backups are done, in this example, at 2:00 a.m.

Backups do not maintain a complete record of e-mail traffic. Backups also do not satisfy regulatory compliance issues. Again, it depends on the industry, but in many cases, regulators do not allow backups. The organization must have an archive of the content. Backups do not provide adequate support for e-discovery. This is due to the cost of searching through backup tapes, extracting the needed information, and so on. Also, backups do not provide employees with access to old content. If it is necessary to search through backup tapes in order to restore a missing or deleted e-mail, this task can be very expensive and time consuming. It typically takes about eight hours from the time an employee requests the retrieval of a deleted e-mail from backup until the time that e-mail is restored. If anyone needs immediate access to e-mail, in most cases, it is not possible when that information is stored only on backups.

Backups provide a snapshot of data, while archiving preserves a continual stream of data. This includes all information leaving the company, whether coming in or sent internally. Backups preserve data, while archiving preserves information. Backups preserve the bits, and that is appropriate for restoring a messaging server. Archiving preserves the context. Archiving preserves data and information that an organization might need for e-discovery. The bottom line is that backups are a tactical solution, but archiving is a much more strategic solution—and one that organizations should follow as a best practice.

## The State of Archiving

What is the state of archiving today? Only about 30% of mid-sized and large companies in North America have a true archiving solution. Based on forecasts, Osterman Research estimates that by 2011, 76% of organizations will have implemented a true archiving solution: one that indexes the content, puts it into archival storage, and makes it possible to search for and extract that information.

Today, many organizations are at a serious disadvantage with regard to e-discovery, regulatory compliance, and storage management, because they do not have archiving systems.

## Recommendations

There is no such thing as an adequate set of recommendations for all companies, because recommendations vary according to the industry in which an organization operates, the size of the company, its past legal history, and so on.

### Understand the Organization's Requirements

Organizations need to understand their requirements and how e-mail is used in the company. Is it accessed as the primary data store? In some companies, it is not. However, in most companies, it is. If an organization is sued, is most of the content that the organization needs to produce for e-discovery tied up in the e-mail system?

### Establish an Archiving Policy

If the organization uses an archiving system, it is important to create an archiving policy. Many organizations have no policies around data retention, data deletion, how long records are to be kept, and so on. It is important to establish a sound archiving policy as the first step. Most of archiving is about policy, not the technology. Organizations have to choose the right technology, obviously, but first they have to establish policies about what kinds of communications to preserve, as opposed to what can be deleted safely. Once organizations decide what needs to be preserved, they need to decide how long it needs to be preserved.

### Archive

Some records need to be kept for a year. Others need to be kept for three, five, or seven years. Some need to be kept indefinitely. Organizations have to preserve records appropriately, based on the industry and many other factors. Organizations need to archive to be compliant with industry regulations. Again, most organizations are not in heavily regulated industries, but some level of regulation must be obeyed to mitigate risk during legal actions. This is the primary reason for most companies to preserve context of communications and to preserve the content itself: to produce it for e-discovery or other legal purposes. It might be necessary to manage storage more effectively. If an organization has a good archiving technology—meaning, one that is scalable and can offload information from the Exchange server readily—then that organization is at a great advantage with regard to storage management. Everything is easier if an organization has a good archiving technology on the back end. It is also important to preserve corporate knowledge.

### Consider the Risks of Failing to Archive

This is a very simple analysis, but if an organization has only a 10% chance that it could face a \$5 million judgment or fine, then that organization can afford to spend \$500,000 on an archiving system, if for no other reason than to break even on the first e-discovery effort. The cost of e-discovery, even for a small company, can be \$100,000, \$200,000 or \$300,000. Most organizations will spend far less than that on an archiving system that will protect them much more adequately than if they just keep backup tapes.

It is also important to consider the intangibles. For example, what happens if an organization cannot produce e-mails appropriately? What happens at trial if the opponent has a copy of an incriminating e-mail but the organization's managers and legal counsel do not have a copy of it? This can result in a loss of reputation. Organizations have been confronted unprepared with their own e-mail in court. Organizations can suffer loss of revenue from prospects that are turned away. Organizations can experience loss of customer goodwill. These are intangibles that are very difficult to quantify and identify, but it is important to consider them. There is far more downside than upside from not having e-mail stored appropriately.

## About Sunbelt Exchange Archiver

For archiving needs, Sunbelt Exchange Archiver (SEA) delivers cost-effective, enterprise-class e-mail archiving for organizations of all sizes, providing administrators with intelligent features such as integrated Hierarchical Storage Management (HSM), Direct Archiving for instant archival of incoming mail, full e-mail

continuity and disaster recovery, and seamless integration with Microsoft Exchange, Outlook, and Outlook Web Access (OWA). SEA combines efficiency and innovation to give organizations a powerful e-mail life cycle management system that offers tamper-proof, long-term storage of e-mails with easy retrieval capabilities and full-text searching. SEA enables companies to preserve all electronic messages on a broad range of storage media, offloading the strain on Exchange servers. SEA provides a cost-effective solution for customers concerned with archiving e-mail for legal, retention, and compliance reasons, as well as significant benefits in terms of reducing the size of the Exchange store. With SEA, our customers are able to better cope with the growing volume of e-mails and gain control over their e-mail management storage costs, while ensuring compliance and increasing performance and efficiency.