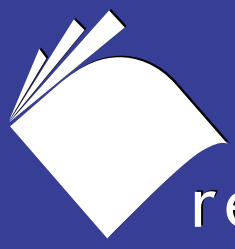

realtimepublishers.com™

The Definitive Guide™ To

Email Management and Security

singlefin
e-mail protection services

Kevin Beaver

Copyright Statement

Chapter 6: Managing Email Effectively

Throughout this book, we've explored several email management concepts—from thwarting off spam to monitoring employees. In this final chapter, the discussion will be more detailed regarding policies, user awareness training, data storage and backups, and data retention as they relate to email management.

Email used to be considered a casual method of communication; email messages are now being treated as true business documents. Email is slowly taking over the fax machine and telephone as the business communication medium of choice. Many organizations would be brought to their knees if their email systems were unavailable. Between the messaging, calendaring, and contact functions, many users simply want and need access to their email practically 24 × 7 in order to function efficiently in their jobs.

Email message stores house the majority of critical intellectual property within today's information systems regardless of the size of the company. As if this burden is not large enough for email administrators to bear, they must now ensure that their organizations adhere to strict federal regulations that affect every facet of email communication.

The retention of emails is becoming an increasing responsibility for organizations thanks, in part, to the corporate misdeeds of recent years in the United States. Larger companies—particularly those that are under intense federal regulation—are taking email retention more seriously. As a result, the need for storage space as well as policies and procedures associated with email retention has become evident. The need to retain file attachments, deal with spam, provide unified message, integrate voice mail, enable access to videos and image files, and the sheer quantity of incoming and outgoing messages is causing many administrators to rethink their email system design and management.

Email Policy Development and Management

Few companies have security policies, and fewer yet have specific policies regarding email. In those organizations that do have policies, the policies often are not enforced. The reason for these shortcomings is a general lack of understanding about the value policies can bring to an organization and a lack of knowledge about how to get started creating and implementing them.

Let's start with the basics. What are policies? In a nutshell, they are statements about how an organization handles the who, what, when, where, and why questions related to email. Policies address such questions as:

- Why is this policy in place?
- Who does it cover?
- What messaging systems are covered?
- Can personal emails be sent/received?
- When is the policy in effect?
- What is considered acceptable email usage?
- What type of monitoring will take place?

- What will happen when a policy is violated?
- Where can users go to get more information?

Why do you need email policies? Email policies can help make users aware of the threats and vulnerabilities associated with email, which, in turn, can prevent security breaches and ensure that organizations adhere to regulations. Policies help lay the foundation for which all technical and business processes related to email are carried out. When upper management sets a good example, they help cultivate a culture in which everyone places a value on email as a corporate asset and works to protect it.

> ☞ It is critical to have a policy committee that includes people from different departments within your organization—such as Human Resources (HR), legal, operations, and upper management. If email policies are coming from only the IT department, the policies will most likely be seen by users as just another technical inconvenience and won't be taken seriously.

> 🕮 Refer to Chapter 4 for more information about employee monitoring.

Policies must be enforceable from an HR and legal perspective, and they must be enforced consistently and across the board. Email policies are more than just documented words. They define critical business processes that must be tightly integrated within every department and function within the organization. Figure 6.1 illustrates an email policy lifecycle.

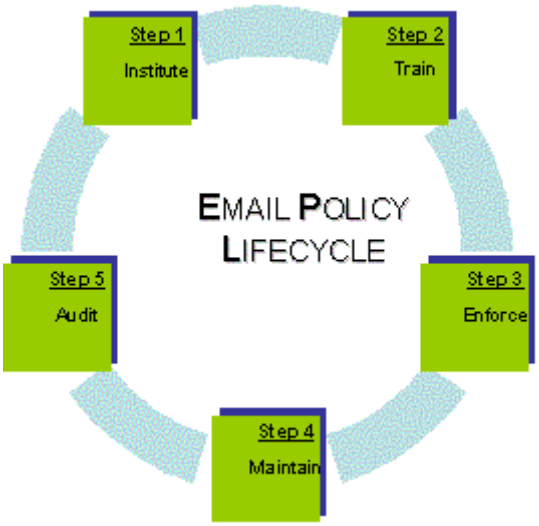

Figure 6.1: The essential elements of email policy management.

There aren't a set number of policies that every organization needs to implement for email; the policies in place should cover topics such as acceptable usage, backups, retention, and so on. The number of policies your organization employs depends on your organization's needs. Email policies should be short, to the point, very high level, and non-technical. In fact, most policy statements can be made in just a few sentences, as the following example email acceptable usage policy shows.

Example Email Acceptable Usage Policy

Introduction

This policy covers acceptable email usage when utilizing company information systems.

NOTE: You might want to include more information here such as the purpose and reasoning behind this policy.

Scope

All users of company information systems.

Policy Statement

Email is intended for business purposes only. All use is subject to monitoring, and there is no right to privacy when using company equipment. No user shall at any time send or store email that contains malware, a warning about malware, unsolicited commercial email, or that is considered pornographic or adult content in nature or would otherwise offend any other user of the system.

Roles and Responsibilities

Each individual user has the responsibility of ensuring adherence to this policy. It is the role of the information security manager to enforce this policy.

Procedures

Content filtering

Logging and auditing

Password protected screen savers

NOTE: You should add more details here or simply refer to another document that details the procedures.

Measurement of Compliance

Email usage is subject to monitoring at any time. Misuse will be assessed using content filtering and log monitoring software as well as by manual inspection.

Sanctions

Anyone that violates this policy is subject to disciplinary action including termination.

NOTE: You'll want to pay special attention to this area based on organizational culture and applicable employment laws.

Review and Evaluation

This policy shall be reviewed and evaluated at least once a year based on its effectiveness, cost to maintain, and impact on business and technical processes. In addition, this policy shall be revised as needed based on newly discovered security risks, security incidents involving email, or any major changes to the organization or information systems.

Related Documents

Acceptable Internet Usage Policy

Incident Response Plan

Revisions

Version 1.0 created August 25, 2003

Policies are only as effective as their weakest link—the users. People either intentionally or unintentionally violate policies. In order for policies to be properly enforced, you're most likely going to need to implement technological controls:

- Email content filtering
- Archiving features enabled in email server and client software
- Automated backups that run every night
- Email software attachment controls

The benefits of these technologies is that they allow more granular control over email messages and thus help reduce the load on human (IT staff and end user) and technical (server and storage space) resources. No one can simply enforce all policies by themselves. A real world example of technological controls is Singlefin's Policy Filter, which allows email administrators to block messages based on size and number of recipients per domain. Figure 6.2 shows these settings.

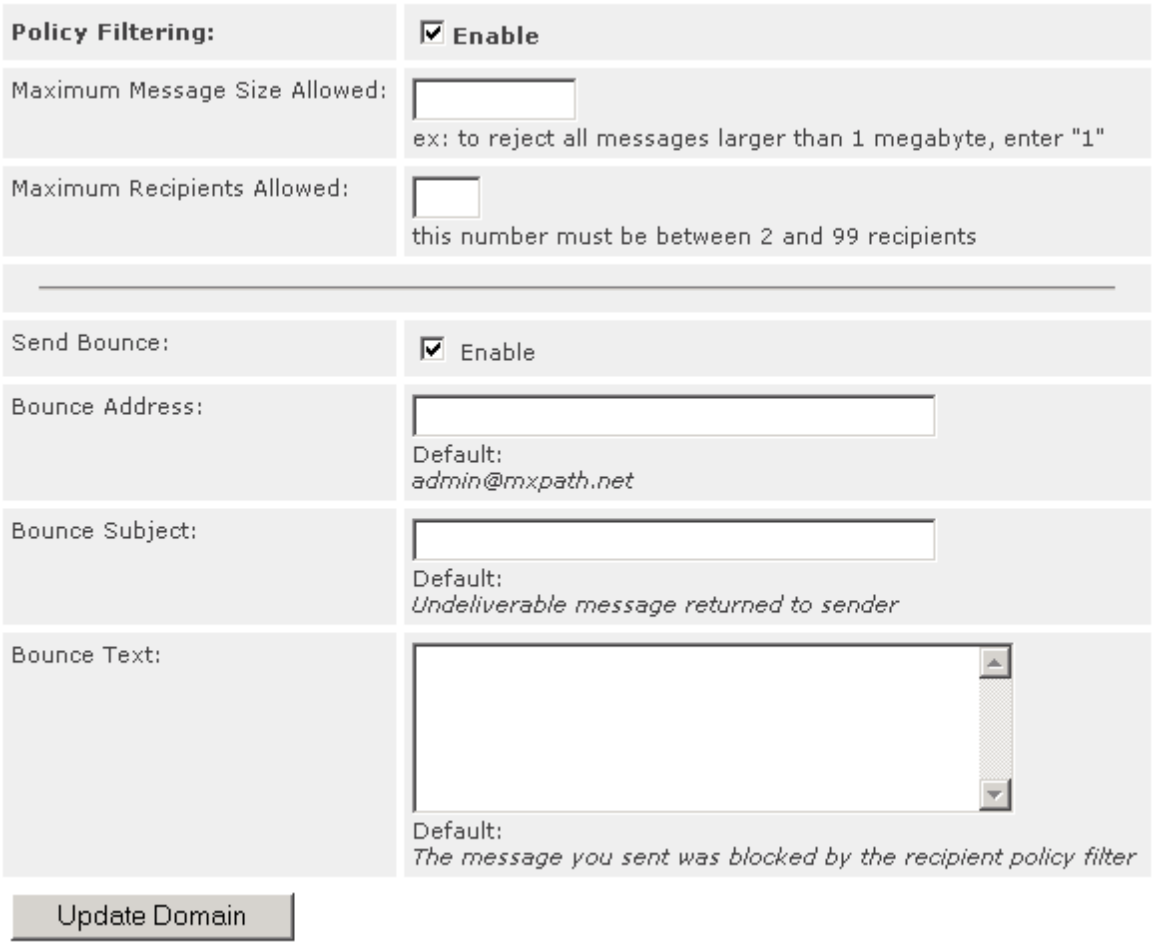

Figure 6.2: Using a third-party product to set and enforce maximum message size and maximum recipients allowed.

Consider buying a policy-management application. They not only allow you to store your policies but can also quiz users about those policies to help you better manage compliance. Similar to the content filtering concepts I discussed in Chapter 4, email policies that are enforced via technical systems can be configured to reject, rewrite, log, forward, redirect, quarantine, hold, send alerts, and even add disclaimers to messages going into and out of your network.

Some email management and security concepts, especially those relating to encryption, are unique to specific industries so it is extremely important that upper management and legal counsel are involved in setting the email usage and policies. For example, there have been court rulings that say sending legal notices via email are legal. Does this affect your company, line of business, or industry? It is very possible, so make sure that the proper expertise outside of IT and security is involved in the decision-making processes surrounding email communications.

The following list highlights tips for developing effective email policies and ensuring that they work for your organization:

- Policies must be enforceable and enforced to the same degree for everyone; otherwise, they are merely advice and an overall wasted effort.
- If you obtain pre-written policies, be sure to customize them to your specific organizational needs.
- In the future, you will think of new policies that need to be created and changes that need to be made to your existing ones. That's OK—policy development and management is a continuous process.
- Consider putting the actual policy statement section of each policy into your employee handbook and get sign off on them from each employee.
- Perform an annual review of your policies to ensure that they are still appropriate for your business and create new ones and revise and remove old ones as necessary.

User Awareness Training

One of the most critical parts of email policy implementation is training your users. Doing so helps communicate secure practices and promotes proper email usage and security within the organization. The best way to get started on user awareness training initiatives is to get buy-in on what you're trying to accomplish with your policies. You (and your policy committee) will always want to make sure that everyone understands what is going on and are kept in the know. If you set clear expectations for users and lead by example, you can establish trust with your users that will make everyone's job easier.

In your training initiatives, first go over each and every security policy so that everyone understands them. You'll also want to train everyone on what to look out for from a security perspective—such as file attachments, strange behavior on their local computers, and a description of social engineering. In addition, it's critical that your users know what to do and what not to do during a security incident. If you perform this training well and often, it will help make all your work designing these policies worthwhile.

Getting Your Message Out

The following list offers various methods to get out your message and ensure that email security awareness stays on the top of everyone's mind:

- Introduce email policies and awareness training concepts during new employee orientation
- Distribute an email survival pamphlet with tips and FAQs for all employees
- Host periodic lunch and learns
- Send out emails or newsletters

Additional tools and trinkets you can used to help with your efforts are:

- Screen savers
- Postings on an intranet Web site
- Posters around the office
- Promotional items such as coffee mugs, pens, mouse pads, sticky notes, and so on. (Check out Green idea at http://www.greenidea.com and Security Awareness at http://www.securityawareness.com for neat screen saver, poster, and trinket products to help with user-awareness initiatives.)

The following list highlights tips to ensure an effective user awareness training program:

- Treat awareness training as a long-term investment in the business and as an ongoing process.
- Ensure that your message is aligned with the specific audience you're addressing.
- Keep your message non-technical.
- Show the business reasons behind the policies.
- Develop incentive programs to help boost effectiveness.

☞ For a useful site about email etiquette, check out http://www.emailreplies.com.

Storage Considerations

Email storage considerations are on practically every email administrator's mind. Loads of spam and file attachments, fancy HTML formatting, and the retention of emails that are no longer needed are causing a storage space nightmare. From a simple workstation that needs a hard drive upgrade to the high service costs involved in adding more space on a storage area network (SAN), messages are overflowing and there doesn't seem to be an easy solution.

Much of this trouble is based on email's growing importance within most organizations. You may recall from Chapter 1 that email is being used in so many new ways:

- Internal business communications among employees
- Fulfilling and tracking sales orders
- Customer service communications
- Research and development collaboration
- Supply chain collaboration with business partners
- Doctors and lawyers corresponding with clients
- Instructors communicating with students about lessons and class assignments
- Owners and managers executing business contracts

The fact that email databases are drastically increasing in size is causing a serious degradation in performance and an increased need for maintenance for email servers and workstations alike. This need ultimately affects user productivity, which generates silent and often overlooked costs.

Outside of the spam epidemic—for which I provided solutions in Chapter 3—perhaps the biggest problem related to email storage space is file attachments. Many people use email for file transfers because it's convenient. A problem develops when users send a file attachment to another user within the same internal network instead of simply sending a pointer to the file such as \\server\public\financials.xls. It is usually much more convenient to just attach the file. However, it's these small changes in email usage that can cause or fix a problem like running out of storage space. Create a policy about attachments and train your users on how to implement that policy.

> Most popular email servers such as GroupWise, Exchange, and Domino store only one copy of an attachment within a domain even if an email is destined to multiple internal recipients. This functionality can drastically reduce the amount of space used by your message store. Check your administrator's guide to make sure this feature is enabled in your system.

Another email storage problem is that most people don't zip or compress files before attaching them to emails. Why? Because it's inconvenient! Consider requiring your users to do so or implement a technology that does so automatically. Many file types—especially plain text, word processing, and spreadsheet files—can add up to substantial storage savings over time when they are first compressed.

There are vendors such as C2C that make products that automatically compress files on the fly without user intervention to help manage mailbox sizes. These products are great for reducing mailbox sizes, lowering network bandwidth usage, and speeding email backups and restores.

An additional solution to your potential or current storage problem is to limit the size of user mailboxes. Typically this is done at the server level as can be seen in the GroupWise server settings in Figure 6.3.

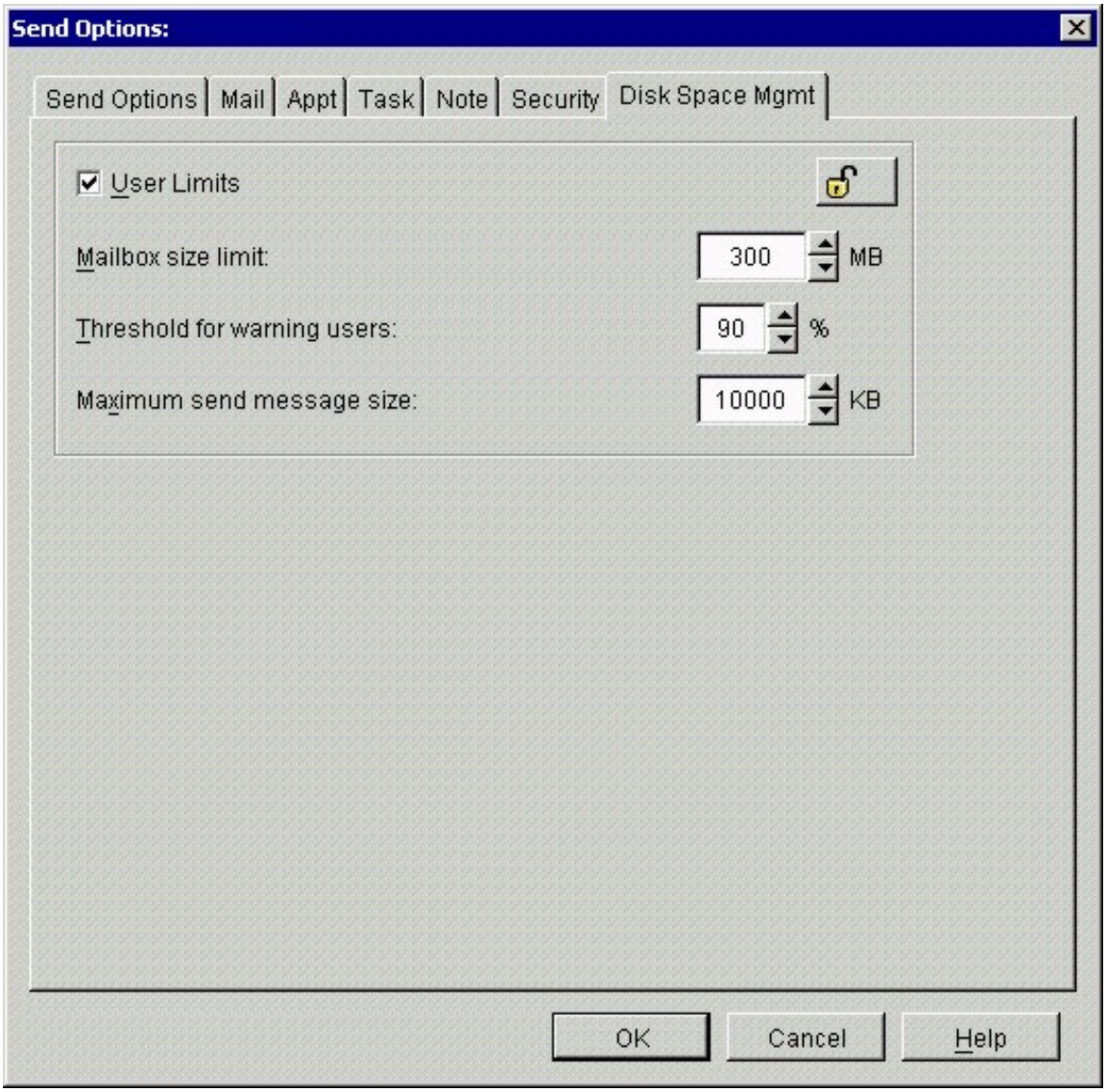

Figure 6.3: Mailbox size limit configuration settings.

Limiting the size of user mailboxes can be hazardous to your health because many users don't like being told they're going to lose some of their emails or that it's going to be less convenient to access saved emails. Mailbox size limitation is a highly charged issue and is best done when you're setting up an entirely new email system from scratch. Make sure upper management is on your side before you go down this bumpy road.

You can also limit the size of user mailboxes by performing (or better yet, having your users perform) routine maintenance on local database files. Some email clients have a "Compact Folders" function to compress the data stored in local inbox files. As a simple test, I compressed the mailbox folders in my Mozilla email client to see what kind of space savings I could achieve. I ended up saving 11MB of space. This might not seem much, but I just ran the Compact Folders function a couple of weeks ago! That's how much slack space had accumulated in a short period of time.

In addition, most email server applications have database maintenance functions that perform checks on the message store to ensure proper operation and to compact the database files. If this is something that you have not done, refer to your email server's administration guide and learn how to perform these checks. It will make your email system run more efficiently and help prevent any email database corruption that could lead to major problems in the future.

Consider limiting the types and sizes of attachments that are sent and received by your email server. Do people really need to send file attachments larger than 10MB? Probably not, but they certainly try. If you have certain users that need large-file-sending functionality, configure your system to permit only those users to do so. Also consider not allowing HTML-based emails because their graphics and formatting codes can take up a considerable amount of space compared with plain-text messages.

Many organizations have users that store their messages locally such as in Outlook .pst files. This may be fine for small organizations, but it simply gets out of hand and impossible to manage for organizations with more than a dozen or so users. In addition, these email databases are more vulnerable when they are spread out on everyone's systems because the data most likely won't be backed up properly.

A quick note on email logging—specifically SMTP logging. SMTP logging can prove to be very beneficial in fine-tuning your email system, tracking email attacks, and determining whether system upgrades are needed, but there's a catch! As with any computer or network logging function, your log files can fill up your free hard drive space in a matter of days—if not hours—if you're not careful. Use logging sparingly unless you have a practically unlimited amount of storage space, and monitor your logs and system stability periodically.

If you think that simply adding new hard drives to your email systems is the solution to the problem of email overload, keep in mind that it is only a short term fix. If you do this, you'll eventually have to add more servers or even external storage devices to the mix, not to mention bigger backup systems, causing your hardware and management costs to drastically increase. It could be time to consider a SAN or NAS device for your network to share amongst all of your systems. You might not need an extremely fast storage solution for email because email is normally not used as a real-time application. A simple iSCSI and ATA drive based system could be more than enough to meet your needs because a lot of caching takes place on the email server itself.

The bottom line on email storage space is that the more space that is saved on an email system, the more efficiently your system is going to run. You can save on disk space, which leads to quicker backups and restores and ultimately lowered maintenance and hardware costs. Doing so will also help ensure your email system is running at its peak performance and will minimize database maintenance and repair times.

Backups

Email isn't just causing a storage nightmare; it's causing problems with backups as well. The myriad data backup options available include tape, disk to disk, optical, and even online backups in which you transfer your data securely across the Internet to an offsite storage facility. You could have a backup system dedicated to email or you could simply backup your email systems as part of the overall system. Table 6.1 shows the common backup types along with their associated pros and cons.

Backup Type	Pros	Cons
Full *Backs up everything*	Easier and faster to restore the entire system in the event of a catastrophic failure	Take more time and requires a large amount of backup media
Incremental *Backs up everything that has changed since the last full or incremental backup*	Faster backup times than full or differential methods	Slow restore times; restores require all backup media since the last full backup
Differential *Backs up everything that has changed since the last full backup*	Faster than full backups and easier and faster to restore than incremental backups	Requires more backup media than incremental backup requires

Table 6.1: Backup types and their associated pros and cons.

> ☞ Some backup software gives you the option to backup the entire email database or back up each user's mailbox (also known as brick-level backups). This usually requires an add-on product specific to your email platform, but can be useful because it can make the discovery process a lot easier when the time comes to search for and restore specific mailboxes or messages.

How often should you back up? The answer depends on how current you need your restored information to be. It could be once an hour, once a day, once a week, and so on. There is not a standard answer because the frequency depends on your organization's specific needs. The following list highlights a few issues to consider when determining how often your email system should be backed up:

- Amount of data to be backed up
- Criticality of email data to the organization
- Email system risks determined during a risk assessment
- Time available to perform backups
- Backup type (full, incremental, differential)
- Backup device (tape, disk, WORM, online replication, and so on)
- Amount of effort required to restore the system if a recent backup is not available

Regardless of the backup medium or method, make sure you perform backups often to minimize recovery time and losses. In addition, keep at least one recent backup offsite in the case of fire or other environmental disaster. You don't want your backups being destroyed along with the data you're trying to protect!

> ☞ Very few organizations encrypt their email backups. This is something you should consider doing given the physical security vulnerabilities associated with tapes, removable disks, and so on.

The following are some email backup policy issues you should consider:

- Purpose of the backups from a legal, business, and technical perspective
- Scope of what's covered
- Frequency of backups
- Type(s) of backups performed (full, incremental, or differential)
- Security mechanisms to protect your backups such as passwords and encryption
- Location and storage of backup media (preferably offsite)
- Creation and maintenance of backup logs

Fault Tolerance

When it comes to fault tolerance, there are various issues you will need to consider. Email has become such a critical tool within today's business environment that hardly anyone can go without it for very long. For a minimum level of fault tolerance, you will want mirrored drives or a RAID configuration in the event of a hard drive failure. Another useful configuration that only adds a few hundred dollars to the cost of your servers is redundant power supplies. I've experienced quite a few server power supply failures over the years—it seems like that is usually the first component to go.

It also helps to have a good hardware maintenance contract in place with your vendors. At the very least, you'll want a maximum one-day turn around time for service. However, 24 hours will

seem like an eternity when you have angry users breathing down your neck because they can't access their email. Go for a 4 hour onsite service contract if it's available and you can afford it. These are pretty typical from most server and storage hardware vendors and are often very inexpensive given the value they provide.

For very critical email systems (those that can't go down at all), integrate high availability into the mix. By this, I mean nothing more than simply installing your email servers in a clustered environment. This is pretty simple to do given that many current server OSs have support for clustering built-in. In addition to clustered servers, you should consider installing redundant storage in the form of a NAS or a SAN. These systems, which can be centrally managed, are a solid component of business continuity and disaster recovery plans, especially for larger organizations that can justify the cost.

Email Retention

Email retention refers to the archiving and management of past business communications. Why would you want an email retention program? This retention, or archiving, of email communications is essential for various reasons—the most important of which is to assist in possible legal investigations (email has become a form of evidence just like any hard copy document). In addition, corporate misbehavior has helped spawn new laws that regulate how long emails need to be kept for certain industries. These regulations include:

- NASD Rules 3010 and 3110
- SEC Rule 17a-4
- Sarbanes-Oxley Act
- HIPAA
- Food and Drug Administration Title 21 Part 11
- Uniform Electronic Transactions Act
- Electronic Signatures in Global and National Commerce
- Federal Communications Commission CFR Title 47 Part 42

In late 2002, the NASD, NYSE, and SEC imposed fines of $8.25M on five brokerage firms that failed to adhere to laws concerning the retention of email communications.

The following list highlights additional reasons to consider implementing an email retention program within your organization:

- Legal reasons
  - Contractual obligations
  - The Internet has no boundaries, therefore there are local, state, federal, and international laws that must be considered
  - Messages can be key pieces of evidence in lawsuits or even simple business disputes
  - Email archives can be used during investigations, especially when information can be cross-checked with other electronic documentation to validate evidence.
  - Provide proof that your organization follows sound email management practices
- Business reasons
  - Adherence with established policies
  - Enable you to determine which messages are important for retention and free up space that is otherwise being taken up by messages that are no longer needed
  - Record of important dates or events
  - Important business "history"
  - Provide a searchable archive that can make users' jobs easier

In 2003, a United States District Court judge ordered the Environmental Protection Agency (EPA) in civil contempt. This derived from a case when email tapes were reformatted and reused after a court order was issued to obtain electronic communications records of contacts made with outside groups by the EPA at the end of the Clinton administration. However, the case was put to rest because the EPA had done everything it could to retrieve the destroyed information.

Archiving must be taken very seriously by managers, executives, and even end users who want to be able to access old emails in the future regardless of the reason. Some messages might have great value to the organization. In addition, emails are being used more in lawsuits. Workstations and servers are even being confiscated so that law enforcement officers can perform investigations.

Similar to many other Internet and technology issues, the law is lagging behind the technology here. There are various United States and European laws that affect email retention. For the most part, these laws require emails to be maintained anywhere from 3 years to indefinitely.

Email retention methods are based on and are not much different than the well-established document retention systems that many organizations already have in place. The key difference is that the electronic version is much more difficult to get a handle on given the amount of data as well as the number of places the data can be located.

Email retention is more than just archiving your Outlook database into a local .pst file.

Another difference from older hard copy document retention programs is that electronic documents contain much more data than paper records. This data, known as meta data, can consist of who created it, creation time, receipt time, draft versions, modifications made, last access time and date, and so on—much more than can be gleaned from a standard hard copy document. This meta data can help prove the message's authenticity and integrity.

The Problem with Retrieval

Practically anyone can save emails, however, when it comes time to retrieve those emails, most people tend to have trouble doing so given the various locations that emails can be stored combined with the unstructured retention systems in use today. This difficultly with retrieval can lead to trouble, especially during a critical legal investigation. Email files requested by court order must be generated in a timely manner not only for lawyers to build their case but also to minimize the chance that the integrity of the data will be compromised—either maliciously or accidentally.

The electronic medium we're now using for communications has complicated the document retention process given the myriad places that emails can be stored inside your network much less outside your network. Locations inside your network could include:

- Email client databases on workstation hard drives
- Temp directories and caches on workstation hard drives
- Home computer hard drives
- PDAs
- Cell phones
- Email server message store
- Mirrored partitions on local servers
- Mirrored partitions on remote data center servers

There is a good chance that emails won't be deleted from every possible location. Once messages are sent, it's hard to control what happens to them—how they're saved, forwarded, printed, and so on—except for organizations that use software from third-party vendors such as Authentica, which offer technologies that allow you to manage what happens to messages after they're sent. However, most organizations don't have a technology such as this in place. Determining exactly where each email has ended up is virtually impossible, especially given that many of the places emails might possibly reside are not under your control:

- ISP logs
- Third-party email provider systems
- Email server
- Local inbox
- Third parties to whom the messages are forwarded
- Tape backup
- NAS/SAN devices

- Online storage
- Hard copy printouts

> ☞ If you change email server or client software, you'll still need to maintain your email archives from the old system. Also, be sure to hang on to the original software media in case you need to reinstall the programs for message retrieval.

Given that email data is as critical as any other type of data in hard or soft copy within an organization, fast search and retrieval times are a necessity. Unfortunately, email administrators are spending huge amounts of time searching for long-lost email messages on behalf of end users or during a court-ordered investigation. Some of these searches, especially the ones involving formal investigations, might go back several years spanning various applications, servers, and storage media. These investigations can cost thousands and sometimes millions of dollars.

> There are systems such as Legato's EmailXtender and KVS' Enterprise Vault that provide email storage and retention management functions that allow for direct access to archived email messages.

Creating an Email Retention Policy

Before you decide on an email retention policy requiring emails to be deleted after a certain period of time, such as every 60 to 90 days, you will need to weigh the pros and cons. Every company has "email hoarders" that keep every email from the beginning of time stored in their inbox. This type of deletion policy will keep all those hoarders in check and help to keep your system running at peak performance. On the plus side, deleting company emails in such a short time period will free up a lot of storage space on your system. On the negative side, do you want to be the one that deletes your CEO's emails or gets rid of correspondence or files that are vital to your company? Are you going to be portrayed as the bad guy when you delete the precious photograph of the HR manager's first grandchild? By keeping to a strict deletion policy, you inevitably will anger some of your users, so be sure that upper management will back up enforcement of such a policy.

> When email retention is left up to end users, they end up making retention decisions on behalf of the organization that might or might not be adequate to satisfy legal requirements.

Furthermore, when you start making decisions about your email data retention policies and methodologies, you will need to take into consideration the concerns of the end user and the email administrator. Your end users are going to have questions such as:

- Who is going to have access to my email?
- How long are they going to keep email?
- Will the organization be storing everything I send or just those emails I receive?

You will also need to address the following:

- What laws affect email retention in my organization?
- How much will email retention cost?
- How much storage space will be required?
- How can I ensure the privacy of my users?
- How long must I store these emails?
- If I choose an offsite storage company, how quickly can we access emails if necessary?

Email Retention Policy Considerations

The following list highlights considerations for your organization's email retention policy:

- Retention timelines for different types of emails—outline the data type and its corresponding retention period
- Which emails must be kept and which must be deleted
- Require users to periodically archive messages (manually or automatically)
- Archiving procedures to acquire emails from inboxes and transfer them into the archive database
- Procedures for discovery requests
- Handling procedures for databases, messages, and media that are under investigation
- Destruction procedures for eliminating messages once expiration has been reached

Enforcing Your Policy

So how can you enforce an email retention policy? User training is a good start, but technological controls are the only sure way of making it happen. Another layer of policy enforcement can be provided by enforcement technologies from companies such as Omniva and Zantaz that can assist in making sure messages are handled properly. Also, various email servers have mailbox management tools allowing administrators and users to easily archive and purge messages based on retention schedules (see Figure 6.4).

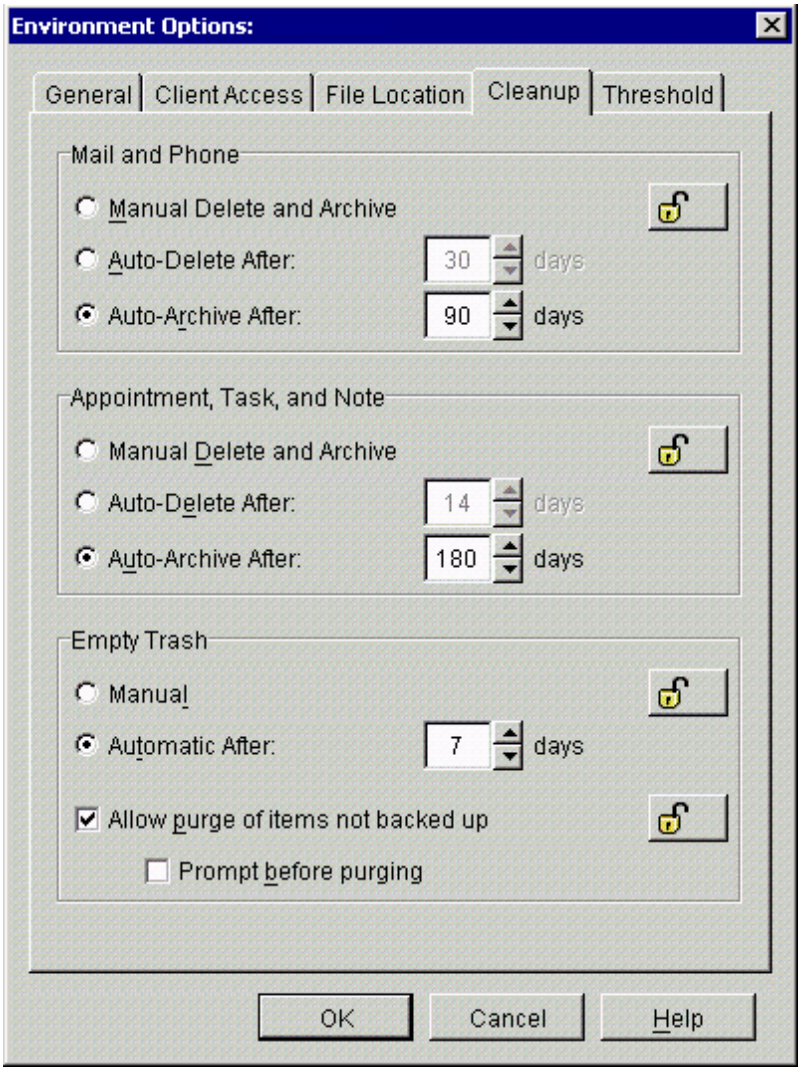

Figure 6.4: An example of email archiving options.

Note that the archive and delete options in Figure 6.4 are for all groupware content including email, phonebook, and calendaring information. Don't forget these other areas as they can take up a considerable amount of space in your message store. Also, these archiving settings are for the entire email domain. This type of centralized management is the best way to configure and enforce specific policies. Otherwise you run the risk of users handling the archiving responsibility and policies not being followed.

If you must leave it up to your users, there are ways they can archive their content stored on each workstation—as can be seen in the Microsoft Outlook settings in Figure 6.5. This policy enforcement method can only realistically be implemented in smaller organizations in which users are trained well and understand the email management and security issues at hand. Otherwise, this method can create even larger email management and retention problems.

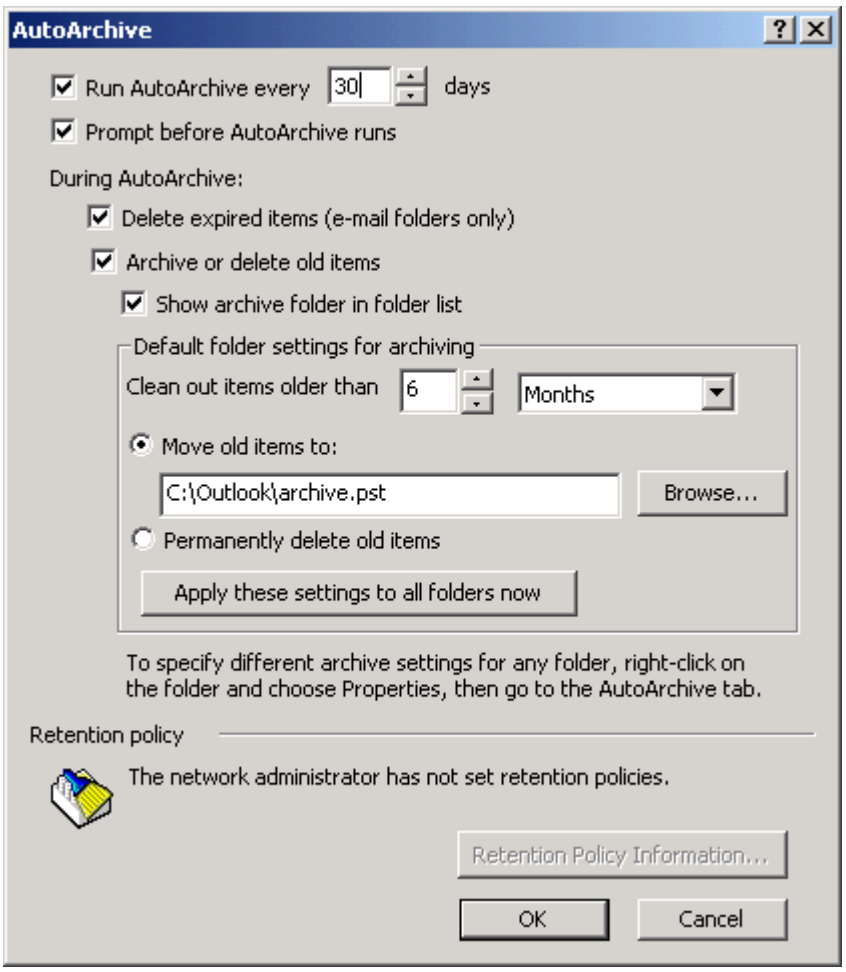

Figure 6.5: Archiving options in Microsoft Outlook 2002.

Note in Figure 6.5 that the option to prompt before archiving is set. You might want to disable this option because users tend to cancel out of any operation that's going to slow down their computer in any way. Also, consider pointing the archive file to a network drive or NAS/SAN storage device that you know will have enough space and will be backed up regularly. And ensure that you have the appropriate security settings on this location—you don't want everyone to be able to browse these files from the network! Also, keep in mind that this archiving function could generate a lot of network traffic that could slow down the network or even perform a DoS condition on the system to which the files are being copied.

Another noteworthy setting in Figure 6.5 is the retention policy. The Retention Policy Information button would be available if this workstation was part of an Exchange domain that has retention policies set similar to the GroupWise settings shown in Figure 6.4. Instead, these settings are for a standalone workstation used for POP3 and SMTP email that doesn't connect to an Exchange server.

Emails that are retained must be housed somewhere—the server, local workstation, tape backup, WORM disks, CDs, DVDs, and so on. You must find a solution that fits your organization's needs.

There are email shredding utilities that store encrypted messages and destroy the key to decrypt them after a certain period of time. These utilities don't actually delete the message, just the encryption keys. You might wonder what value this might provide other than eliminating email you don't want others to see. Well, there's a possibility that it can actually serve as a forensic record for email retention and auditing purposes. Key management is critical here. If the encryption keys are lost or the pass phrases are forgotten, it's the same as having no email archives at all. It doesn't make sense to keep messages that can no longer be decrypted either.

> ☞ Don't forget the security of your email retention system. These systems and data need to be protected as one of the most critical assets within the organization.

A simple deletion of email messages might not suffice as there's a chance they can be recovered using some simple forensics tools. The United States Department of Defense 5015.2 standard outlines how to safely delete data so that it cannot be recovered.

> ☞ Keep your eye on the IETF Message Tracking Protocol charter. These emerging standards could, among other things, serve as an add-on to an email retention program because they provide message tracking and routing information. You can get more information about this emerging standard at http://www.ietf.org/html.charters/msgtrk-charter.html.

An email management system can help lower the overall cost of managing your email system as well as ensure that email system availability is maximized. This could be accomplished by:

- Providing users with the ability to access their own archives making users more efficient at their jobs as well as offloading tasks that the IT department would normally handle
- Helping to reduce storage space requirements
- Allowing for quicker recovery from email system disasters
- Allowing for faster access to archived messages
- Functioning as a traditional records management system that is dedicated to managing emails throughout their lifecycle

The following list highlights tips for implementing an effective email retention program in your organization:

- Your two main goals are to have messages that are well organized and easily accessible.
- Whatever solution you choose must fit within and operate well with your existing email and IT infrastructure.
- Ensure that users can easily retrieve their own messages if needed so that IT resources are not unnecessarily drained.
- Utilize spam and content filtering systems to purge the junk before it makes it to your email system. If residual junk messages get past—and they will—instruct users to delete them immediately to minimize storage and management overhead.
- Make it policy to regularly remove unimportant messages such as personal emails and newsletter subscriptions.

- It's critical to segregate the various email data types—based on your data classifications—into their own archives to ensure that the messages are kept long enough and aren't kept longer than needed. Otherwise, you'll end up having to manage more archive data and media, which will, in turn, make message retrieval slower and more costly.
- Make it policy to file business correspondence in its appropriate location (private folders, public folders, and so on).
- Capture entire email messages in their native format so that they can be reloaded in their original applications. The original format tends to hold up better in court.
- Many courts have found that hard copy printouts of emails don't hold much weight because there is no way to verify the meta data found in the electronic version (such as time of creation, time of receipt, modifications made, and so on).
- Look for a software solution that can capture messages automatically without user or administrator intervention.
- Some email capture and archiving applications cannot be turned off, even by an administrator or corporate executive. Consider one of these solutions, as it would prove that your system was not bypassed.
- Capture messages in both inbound and outbound directions whenever possible.
- If you have the funds available, consider purchasing a system that allows you to recover individual emails and attachments without spending enormous amounts of time searching through every message.
- Make sure your retention policy adheres to any applicable local, state, federal, or international laws.
- A retention policy must make good business sense for the organization. A risk assessment and cost/benefit analysis will help you determine whether it should be a concern.
- The more tightly integrated email retention is with everyday business practices, the easier it will be to retrieve and manage email if it comes time to present email as evidence in court.

> ☞ Email databases contain information that is rarely tapped into other than for the occasional restore or discovery request. However, this information can provide an enormous amount of correlation data to help improve business processes such as customer service, marketing, or even assist in investigating email security incidents.

Tools and Resources

The following list provides resources related to email management as well as links to technical information about email and data retention standards.

Email Policies

Bindview Policy Compliance Solutions at http://www.bindview.com

Email-policy.com at http://www.email-policy.com/

Information Security Policies Made Easy by Charles Cresson Wood at http://www.netiq.com

NetIQ VigilEnt Policy and Compliance Management at http://www.netiq.com

SANS Security Policy Project at http://www.sans.org/resources/policies

The ePolicy Institute's books, FAQs, and other resources at http://www.epolicyinstitute.com

Email and Data Retention Standards

ISO 17799—Code of practice for information security management at http://www.iso.ch

ISO 15489—Records management at http://www.iso.ch

Email Backup, Storage, and Retention Vendors

BakBone at http://www.bakbone.com

C2C at http://www.c2c.com

Computer Associates at http://www.ca.com

Educom TS at http://www.educosmts.com

EMC at http://www.emc.com

IBM at http://www.lotus.com

Iron Mountain at http://www.ironmountain.com

Network Appliance at http://www.netappliance.com

eManage at http://www.emanagecorp.com

iLumin at http://www.assentor.com

IXOS at http://www.ixos.com

KVS at http://www.kvsplc.com

Legato at http://www.legato.com

Omniva at http://www.omniva.com

Symmetricom at http://www.exchangeproof.com

VERITAS at http://www.veritas.com

Zantaz at http://www.zantaz.com

Summary

In this chapter, we explore email policy development and management and user awareness training. These two key elements are dependent on each other and can both help make your email management efforts successful. In fact, increased awareness of the business and technical issues associated with email management will help drive policy acceptance and associated technologies forward. The overall goal of effective email management is to classify the various types of email data; document the creation, receipt, and handling of messages; and enable the archiving and/or deleting of messages based on sound organizational policies. Therefore, it is critical to ensure that user awareness training is made part of ongoing business operations.

In addition, in this chapter, we touched on email storage issues including data backups and fault tolerance. The barrage of messages into and out of email systems is only going to grow, so the only practical solution is to handle the growth using solid data management techniques.

Finally, I covered email retention in depth from an IT perspective, including the various policy issues associated. The lack of data ownership and responsibility makes data retention very difficult. Therefore, it's important to classify data, define ownership, and set clear policies and procedures to ensure that it is managed properly. If archived messages cannot be safely retrieved, there is no purpose in performing retention. As time progresses, the market will push vendors for easier and cheaper solutions to help manage email retention. Increased integration with email security products such as malware, spam, and content filtering applications will be necessary to ensure that email storage and retention issues are addressed in a manageable way long term.