realtimepublishers.com™

The Definitive Guide™ To

Email Management and Security

singlefin
e-mail protection services

Kevin Beaver

Copyright Statement

Chapter 4: Email Content Filtering

Content filtering is one of the latest sexy buzzwords that we see and hear a lot about in IT. But what does it really mean? In a nutshell, content filtering describes the technologies and procedures required to permit or deny specific types of data from entering or leaving a network. In its most basic form, content filtering allows or disallows email or Web traffic via basic firewall rules. On the other end of the spectrum, content filtering could go as far as analyzing keywords or phrases within an email, determining what context they're in, and, based on additional factors, stripping the sensitive words out of the message before sending it on to its destination. As Figure 4.1 illustrates, there are four generic types of content filtering.

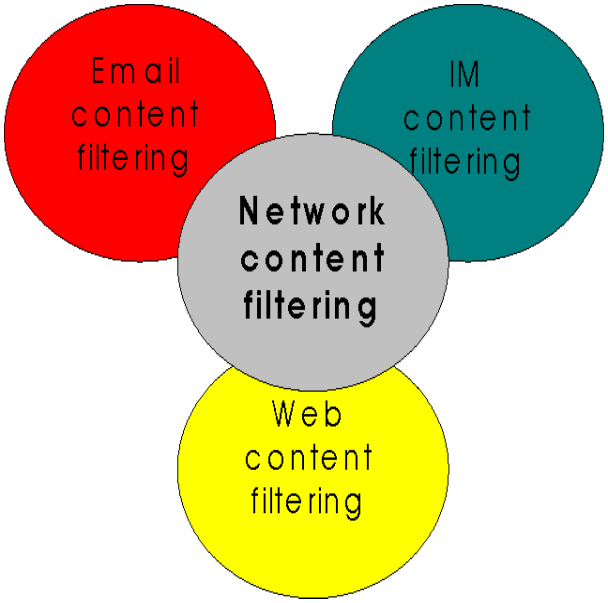


Figure 4.1: The general categories of content filtering.

There is Web content filtering, which consists of filtering specific Web sites based on type of content, URL, domain name, or IP address. There is email content filtering, which consists of filtering malware, spam, and other miscellaneous content. It is this type of filtering that we will explore in this chapter. There is a newer form of content filtering that revolves around instant messaging (IM); this type of content filtering is very similar to email content filtering, so although we won't cover IM filtering specifically, many of the concepts, technologies, and policies that we will cover in this chapter can apply to IM content filtering as well.

Finally, there is a general category of content filtering called network content filtering that helps ward off specific network attacks including DoS, malformed packets, application-level attacks, and so on. These technologies are built-in to most firewalls and intrusion detection systems and are often found in Web, email, and IM content filtering applications.

In Chapters 2 and 3, I focused on specific malware and spam solutions. Those are technically considered content filtering solutions. However, in this chapter, we're going to explore email content filtering from a different perspective. We will look at the email content that's often forgotten about—proprietary, confidential, or offensive material that makes up the email message body or file attachments (see Figure 4.2).

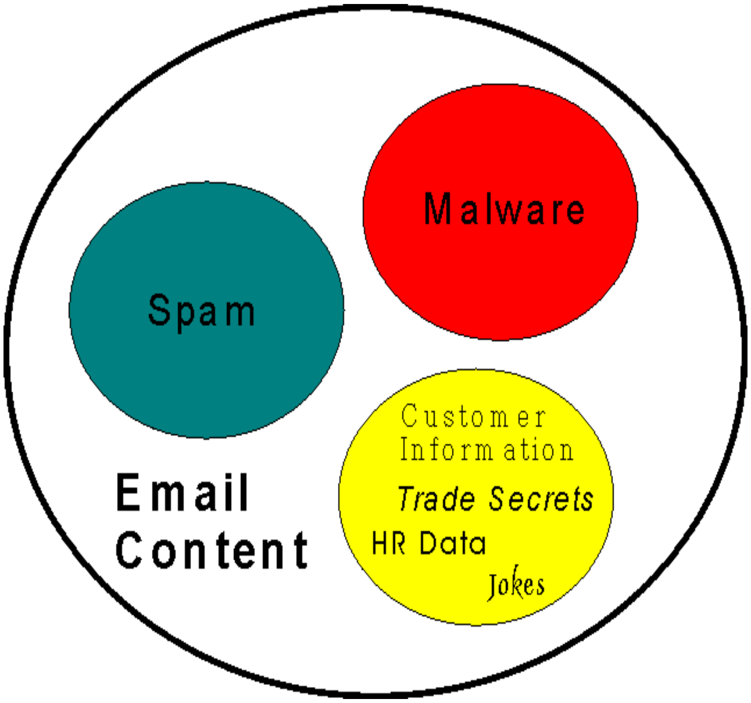


Figure 4.2: The various types of email content.

It's important to keep in mind that many content filtering solutions are part of a larger email security application that also contains malware and spam protection. The content filtering concepts that I'll be discussing in this chapter apply to both standalone and all-in-one solutions. In this chapter, I will cover:

- Risks of not properly content filtering email
- What content should be filtered in emails
- The various ways to implement content filtering within your email system
- The pros and cons associated with content filtering including employee privacy concerns
- Specific content-filtering policies that need to be in place
- Where content filtering is headed in the future
- Content-filtering tools and other resources

Email content filtering is a key business tool that helps prevent questionable material from being communicated via email, protect proprietary corporate information, filter out unproductive personal information, and block adult or other undesirable content from entering your network.

> When it comes to email usage, organizations have two choices—completely trust every action of every employee at all times or implement specific security and control measures to help ensure that bad things don't happen whether they are malicious or unintentional. Email content filtering solutions provide organizations with the ability to limit the use of email systems.

Over the past several years, there have been many legal actions—and, in turn, many organizations put in the headlines—as a result of questionable or illegal content contained in email messages. The U.S. Department of Justice filed a case against Microsoft that was brought on in part by internal emails at the organization. The Enron and Worldcom debacles involved sensitive emails as well. The bottom line is that unless certain content filtering measures are in place, there's really no way to tell exactly what's entering, leaving, or traversing your network.

There are various debates with regard to employee versus employer rights when it comes to monitoring and filtering email. I will cover this subject later in this chapter.

The interesting thing about email content filtering is just how little it occurs. According to the 2003 E-Mail Rules, Policies and Practices Survey conducted by the American Management Association, The ePolicy Institute, and Clearswift, 52 percent of the 1085 respondents said they perform some type of email monitoring on their employees. This slight majority of those who filter is actually much greater than what I've seen occurring in small to midsized businesses.

A couple of major drawbacks to content filtering include the need to place the utmost trust in the content filtering administrator and the fact that there can be many false positives that cause legitimate content to be filtered.

In those organizations in which content filtering does occur, how is it being done? The most obvious way is through content-filtering technologies that I will outline later in this chapter. Although these technologies seems to be the most reasonable and effective approach, based on the same AMA survey mentioned earlier, apparently the average organization relies on employee education as their main form of filtering. Although employee awareness is extremely important, it cannot be solely relied upon as an effective solution. Figure 4.3 shows the tools that organizations use on average to control employees' written email content.

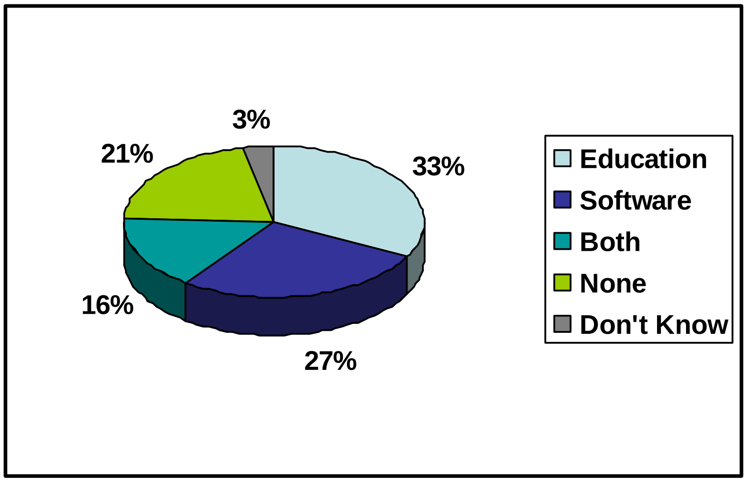


Figure 4.3: Tools organizations use to control employees' written email content (Source: AMA 2003 Email Rules, Policies and Practices Survey).

Although the numbers depicted in the AMA survey have certainly increased since email became widely popular close to a decade ago, the numbers are lower than one would expect given what's at stake.

What Is at Risk?

In Chapter 1, I covered the various threats and vulnerabilities related to email. Given the importance of those email risks, this information deserves repeating. If proper content filtering is not implemented within an email system, there is certainly a lot at stake. Important information can leave your network in the form of regular email messages as well as email file attachments such as Word processor documents, spreadsheets, presentations, databases, and so on.

☞ Proper implementation and monitoring of content filtering solutions can make all the difference in the world for a business. It can help provide a layer of protection for both malicious and accidental misuse.

This silent mischief usually goes unnoticed in the realm of ones and zeros. The scary part is that the loss of important company information can happen with minimal effort. These resources are drained slowly and quietly, which can add up to tremendous losses over time. Given email's utility in today's business, it's very simple for a somewhat determined insider to send out practically all company data via email and never get caught.

✎ The following high-profile cases involving some famous email content mishaps say it all:

Brokerage firm Merrill Lynch settles charges for $100M in May of 2002 after New York State Attorney General Eliot Spitzer pursues them on Conflict of Interest charges based on confidential email content that was leaked outside the organization.

In a case that was filed in November 1996, printing company R.R. Donnelley and Sons is facing a $500M discrimination suit involving emails that were allegedly racist in nature. Black employees claim they were discriminated against when the company arranged transfers after the closing of a plant in 1993. Email documents listing sexual, racial, and ethnic jokes said to be created at their Lancaster, PA plant were presented as evidence in this case.

Chevron had to pay $2.2M in damages to four female employees for sexually harassing emails that were sent via the company email system.

So what exactly is there to lose if email content is not properly filtered? There are several important business- and employee-related issues to consider:

- Loss of trade secrets
- Loss of confidential information
- Financial losses related to bad publicity
- Untimely financial disclosures to the public
- Copyright violations
- Employee productivity losses as a result of sending/receiving inappropriate emails, mistrust, and media attention—not just with the person(s) directly involved, but all employees within the organization
- Sexual harassment liabilities
- Employees "cyberstalking" other people
- Organization's reputation

- Management's reputation
- Loss of customer loyalty
- Human resources (hiring, firing, and so on) costs
- Legal liabilities incurred from libelous comments made about customers or competitors, illegal material, or information such as jokes or pornography that are offensive to employees or other system users
- Failure to meet government regulations
- Legal costs defending these cases
- IT costs researching what happened, purchasing new products, and further securing systems
- Costs as a result of increased network bandwidth, storage space, and administrative requirements

> ✎ Given the numerous areas of potential loss, there are some obvious benefits of content filtering that you can use to sell the idea to upper management. These include:
>
> —Assurance that systems are in place to protect proprietary and confidential information
>
> —Ability to monitor how intellectual property is being used and transferred within the organization
>
> —Ability to monitor how computers and employee time are being utilized
>
> —Protection of business interests
>
> —Proof that the organization has performed due diligence to protect against legal liabilities
>
> —Enforcement of organizational policies and government regulations
>
> —An increase in employee productivity and ultimately morale if executed properly
>
> —Minimize impact on network bandwidth and storage space
>
> —Help control email system security breaches and other misuse

What Should Be Filtered

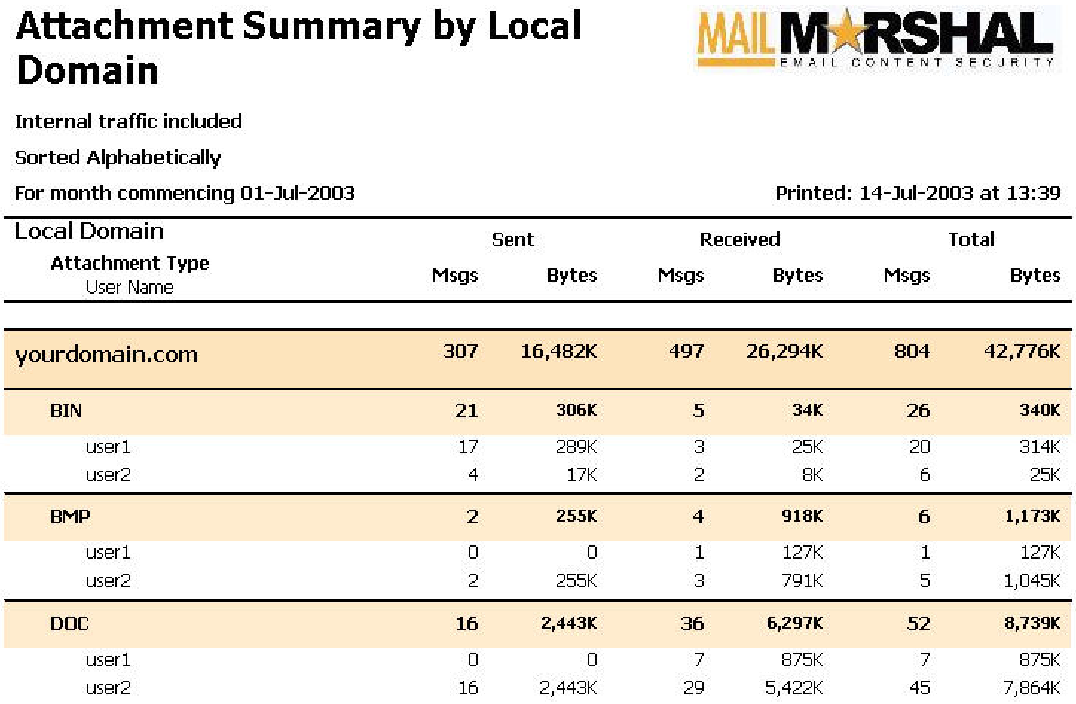
Besides the obvious need to filter malware and spam, you will need to determine what information needs to be protected and at what level. Simply put, you cannot protect that which you are not aware of. You can start determining what needs to be filtered through a process of data classification. It's critical to understand the various types of data that exist on your network and in hard copy form within your organization that could be transmitted via email. Beyond that, you will need to perform an overall information risk assessment to determine other threats and vulnerabilities inherent in your email system.

> 📖 I will discuss data classification as part of overall information risk assessments in more detail in Chapter 5.

An information risk assessment will also help to determine which types of behaviors are occurring on your network so that you have a baseline from which to start. You might find out that you don't need email content filtering—although, that's not likely! This initial behavioral analysis can be done via simple log analysis. That is, perusing your email client and server log files for information about who is doing what. However, this task is not easy or practical. Probably your best option is to run a trial version of one or more of the content filtering solutions that you're thinking about purchasing. Most vendors allow you try their products for a few weeks before making a commitment. All it takes is a simple registration, sometimes a download, possibly some low-end hardware setup, and minimal configuration of one of the products or services to get the ball rolling.

> 🕮 Refer to the Tools and Resources section at the end of this chapter for links to some popular email content filtering solutions.

The type of information gleaned from 1 to 2 weeks of running a trial version of your favorite content filtering application(s) to see what's going on inside your network should provide plenty of ammunition to help create the case for email content filtering. Most email content filtering solutions are easy to install, configure, and run reports from. For instance, check out the email attachment summary information that was easily gleaned from the NetIQ MailMarshal (see Figure 4.4).



Attachment Summary by Local Domain

MAILMARSHAL EMAIL CONTENT SECURITY

Internal traffic included

Sorted Alphabetically

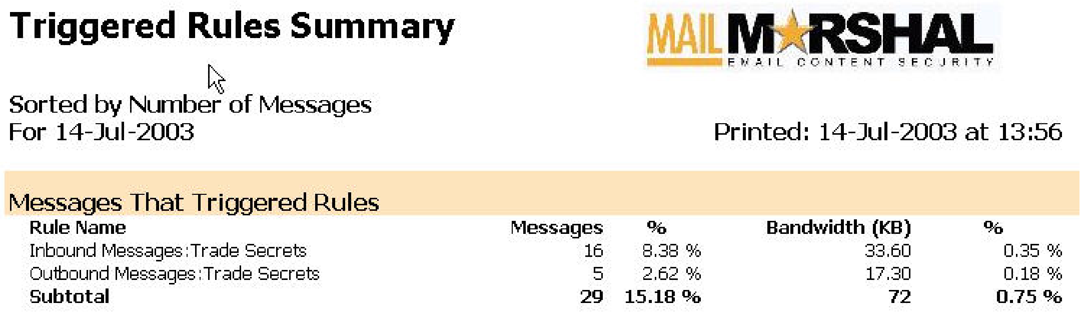
For month commencing 01-Jul-2003

Printed: 14-Jul-2003 at 13:39

Local Domain Attachment Type User Name	Sent		Received		Total	
	Msgs	Bytes	Msgs	Bytes	Msgs	Bytes
yourdomain.com	307	16,482K	497	26,294K	804	42,776K
BIN	21	306K	5	34K	26	340K
user1	17	289K	3	25K	20	314K
user2	4	17K	2	8K	6	25K
BMP	2	255K	4	918K	6	1,173K
user1	0	0	1	127K	1	127K
user2	2	255K	3	791K	5	1,045K
DOC	16	2,443K	36	6,297K	52	8,739K
user1	0	0	7	875K	7	875K
user2	16	2,443K	29	5,422K	45	7,864K

Figure 4.4: Example report about email file attachment activity.

Also, within just a few minutes you can use MailMarshal to create a rule to filter specific trade secret words on inbound and outbound messages, then run a report to see exactly what your users are doing (see Figure 4.5).



Triggered Rules Summary

Sorted by Number of Messages
For 14-Jul-2003

Printed: 14-Jul-2003 at 13:56

Messages That Triggered Rules

Rule Name	Messages	%	Bandwidth (KB)	%
Inbound Messages:Trade Secrets	16	8.38 %	33.60	0.35 %
Outbound Messages:Trade Secrets	5	2.62 %	17.30	0.18 %
Subtotal	**29**	**15.18 %**	**72**	**0.75 %**

Figure 4.5: Example report about emails sent/received containing corporate trade secrets.

Once you determine the need for content filtering, you'll want to determine the specific types of email content to filter. The following list provides a few of the high-level categories:

- Sensitive information
    - Business plans
    - Corporate trade secrets
    - Customer contact database
    - Customer credit card, social security number, or other private information
    - Employee salaries
    - Product plans
    - Software source code
    - Technical product specifications
- Possible junk mail (not necessarily spam, but network hogs and productivity hindrances)
    - Chain letters
    - Chat forums
    - Commercial mailing lists
    - Email newsletters
    - Gambling pool messages
    - Music files

- General keywords and phrases
    - Adult
    - Arts and entertainment
    - Computer hacking
    - Drugs
    - Gambling
    - Job searching
    - Racist
    - Sexist
    - Shopping
    - Sports
    - Travel
    - Violence

> According to content filtering vendor ZixIt, 30 percent of all email messages sent out by a typical healthcare organization contains sensitive information, and 16 percent of these messages contain protected health information (PHI) that must be secured according to the HIPAA legislation.

There are various ways you can filter emails for specific content. From the sender's address to a keyword in an attachment, there are several methods available:

- Sender's email address, domain name, IP address
- Receiver's email address, domain name, IP address
- Direct SMTP or POP3 connections to email servers other than your own
- Email header information such as the sending server's hostname or software version
- Email subject line
- Specific keywords or phrases in the message body or file attachments
- How phrases or sentences are structured
- Length of sentences and words
- Email construction (HTML, text, and so on)
- Character sets
- Alignment and composition of graphic images
- Specific HTML tags
- Hyperlinks
- Embedded scripts such as JavaScript or VBScript

- Type of file attachments
- Name of file attachments
- Email size
- Number of emails sent from a specific host within a certain time period

A range of content-filtering tools and techniques are available to filter on these types of email characteristics. Some content filtering products/services are more feature rich than others, so make sure you do your homework and compare the features that you need with the features that the product/server you're considering actually has to offer. The main objective is for you to be able to maintain full control over your email system.

> One of the biggest content filtering mistakes is to filter only inbound messages. The filtering of outbound messages is just as critical. It's easy to do, so make sure that you enable both inbound and outbound filtering as soon as possible.

How Content Filtering Works

Generally speaking, email content filtering works by comparing the contents of an entire email message with a set of predefined rules that state whether the content (or the entire message) are allowed to pass into or out of the network. Most content-filtering servers function as email gateways similar to typical spam filtering servers. If an email passes through the content-filtering system and there is a match to any of the rules, the application responds in a certain way that is usually controlled by the content-filtering administrator.

The filtering responses can range from silently logging the message and letting it pass untouched, stripping the message of the content that is discovered (as depicted in Figure 4.6), replacing the content that is discovered, redirecting the message to the administrator or a quarantine queue for further analysis, or simply rejecting the message altogether.

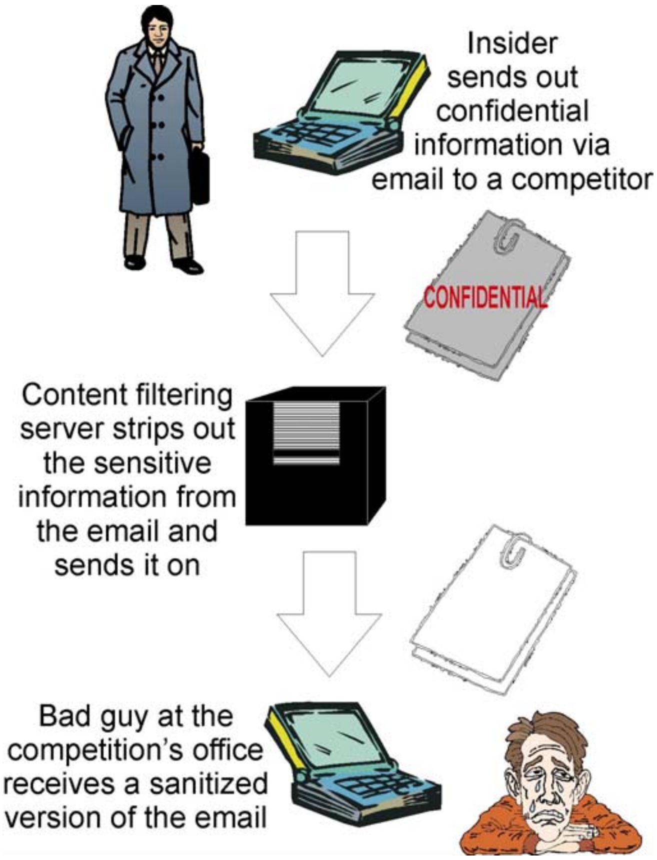

Insider sends out confidential information via email to a competitor
CONFIDENTIAL
Content filtering server strips out the sensitive information from the email and sends it on
Bad guy at the competition's office receives a sanitized version of the email

Figure 4.6: Content-filtering application sanitizing an email in transit.

The key to effective content filtering is to separate the legitimate content from the inappropriate content. When this action doesn't take place correctly, false positives—or improperly filtered messages—will occur. This mishap often requires some form of expert analysis to look beyond simple keywords and actually determine the purpose of the message.

> Certain email content-filtering applications, such as the solution from Singlefin, can filter content based on preconfigured policies within the application, then trigger a specific action. For example, suppose an organization that must comply with the HIPAA legislation receives an email from a known business associate and that email contains confidential PHI. The content-filtering solution could invoke a process whereby the email will automatically be converted to an encrypted link and sent on to its destination or even rejected altogether.

Certain content-filtering products, such as Vericept's VIEW, use linguistic and mathematical analysis to determine not just the content but the context of communication. This technology analyzes the actual code behind the content that is displayed and looks for certain anomalies that are characteristic of questionable content. Some products, such as SurfControl's E-mail Filter, analyze specific keyword combinations to identify sensitive email messages. These types of analysis can help reduce false positives and increase filtering efficiency.

Some content-filtering systems use file signatures to check for specific files entering or leaving the network. The effectiveness of this tracking method depends on whether a highly reliable hash algorithm, such as MD5 or SHA, is used or the tool simply relies on basic checksums.

Other content filtering systems take advantage of existing email traffic logs that are located in various places on your network and beyond. These logs can be stored on the client, on the content-filtering server, on the email server, on backups, in proxy server caches, at the ISP, and on the recipient's network. Keep this in mind when it comes time to track specific email content.

Another content-filtering issue to keep in mind is that emails are easy to spoof and, therefore, certain content may not be properly authenticated. Content filtering needs to work not separate from, but in conjunction with, other information security measures such as authentication systems, access controls, firewalls, and so on. A layered security approach applies to content filtering just as much as with any other information security function.

✎ What about Carnivore? The FBI's Carnivore application, now called DCS1000, which is nothing more than a customized network analyzer, has raised many an eyebrow since its introduction. According to a statement in 2000 made by FBI Assistant Director Donald M. Kerr, "It works by 'sniffing' the proper portions of network packets and copying and storing only those packets that match a finely defined filter set programmed in conformity with the court order." This technology supposedly limits what can be viewed by federal agents to that mandated by court order. Check out the following link to a graphic that provides more details about how it works at http://www.fbi.gov/hq/lab/carnivore/carnlrgmap.htm.

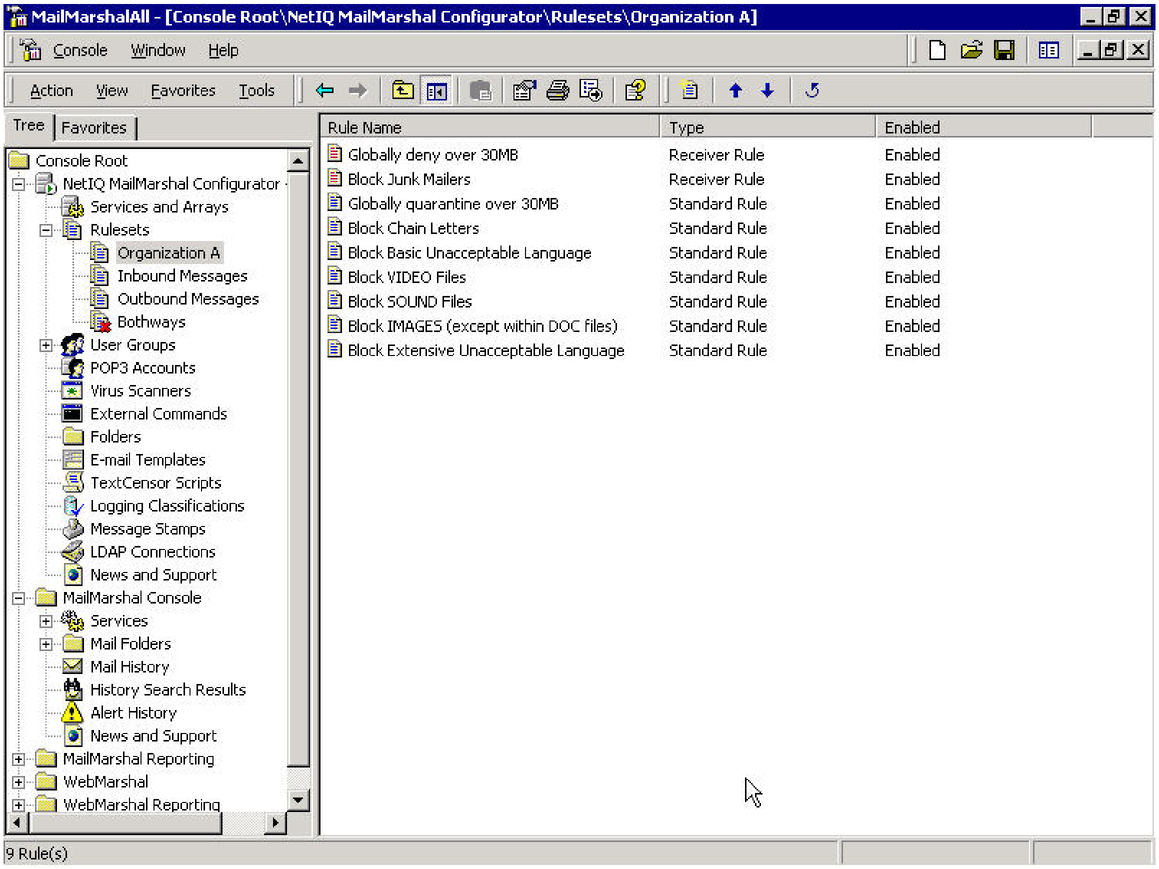
✎ For detailed information about DCS1000, including a link to an independent review of the Carnivore system, check out the following Web sites: http://www.carnivorewatch.org and http://www.epic.org/privacy/carnivore/foia_documents.html.

Content Filtering Applications

Content filtering can be implemented in myriad ways. There are basic client-side solutions built-in to Microsoft Outlook, Mozilla Mail, and Eudora. You can also get content-filtering support from personal firewall/IDS programs such as ISS's BlackICE and Symantec's Norton Personal Firewall. Although I'm not focusing on client-based content-filtering solutions, there is one client-based content-filtering solution that deserves mentioning—Spectorsoft's eBlaster and Spector Pro. These programs can, among other things, provide stealth email monitoring and keyboard logging.

Moving on to network-based solutions beyond the client, there are three main types of content-filtering applications:

- Server applications—These applications include those that are integrated with your existing email server software as well as standalone applications that run on a separate and dedicated server. The content-filtering function may be combined with malware and spam protection as well. These systems can also come in the form of a dedicated hardware appliance. No matter what the hardware requirements are, dedicated content filtering servers and appliances serve a better role in creating a more layered approach to content security. They help offload the content-filtering overhead requirements from email servers and can simplify the management content-filtering function. They also eliminate the possibility of posing a single point of failure in your email environment. Some of the content filtering options available in server applications can be seen in Figure 4.7.

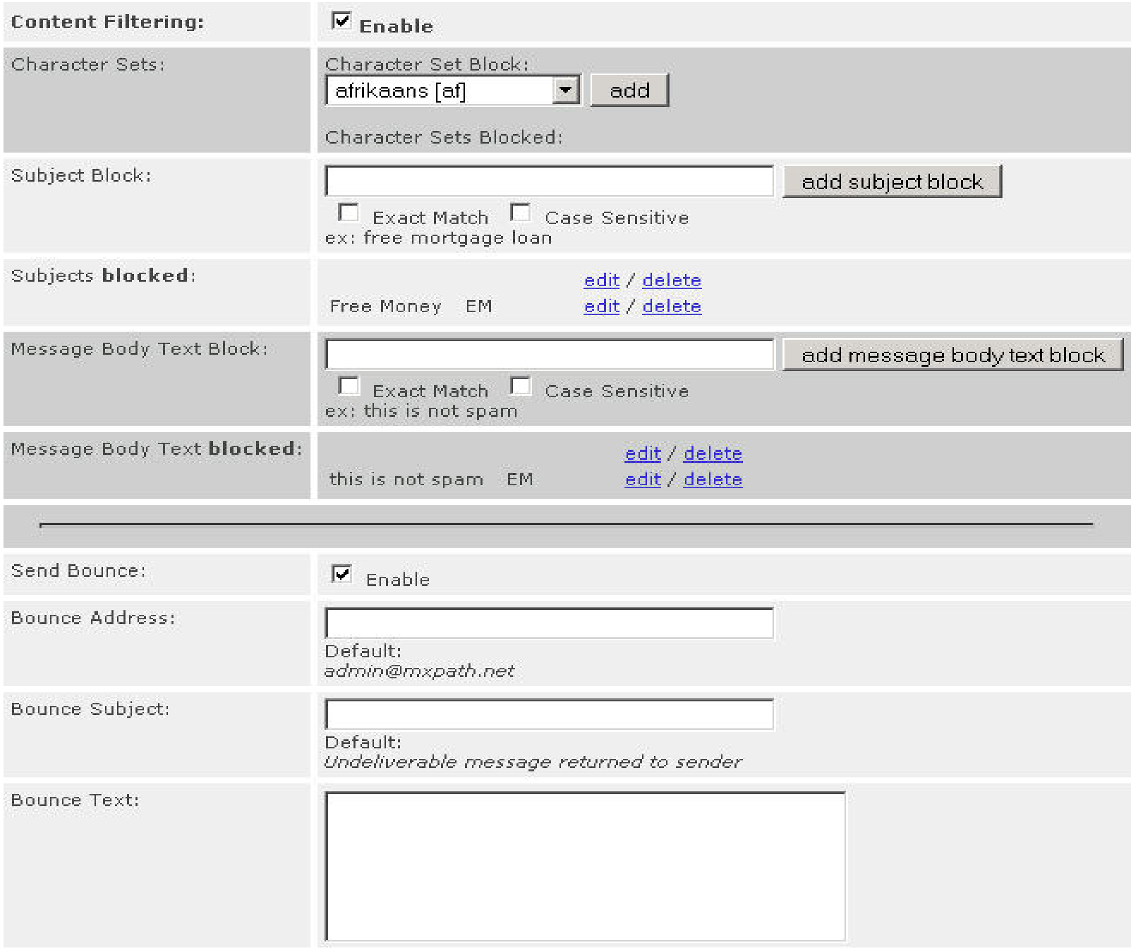


Rule Name	Type	Enabled
Globally deny over 30MB	Receiver Rule	Enabled
Block Junk Mailers	Receiver Rule	Enabled
Globally quarantine over 30MB	Standard Rule	Enabled
Block Chain Letters	Standard Rule	Enabled
Block Basic Unacceptable Language	Standard Rule	Enabled
Block VIDEO Files	Standard Rule	Enabled
Block SOUND Files	Standard Rule	Enabled
Block IMAGES (except within DOC files)	Standard Rule	Enabled
Block Extensive Unacceptable Language	Standard Rule	Enabled

Figure 4.7: Some of the filtering options in a content-filtering product.

> ☞ The more services—such as content filtering, spam, and malware protection—you can run on dedicated servers, the better off you will be from a security and system availability perspective.

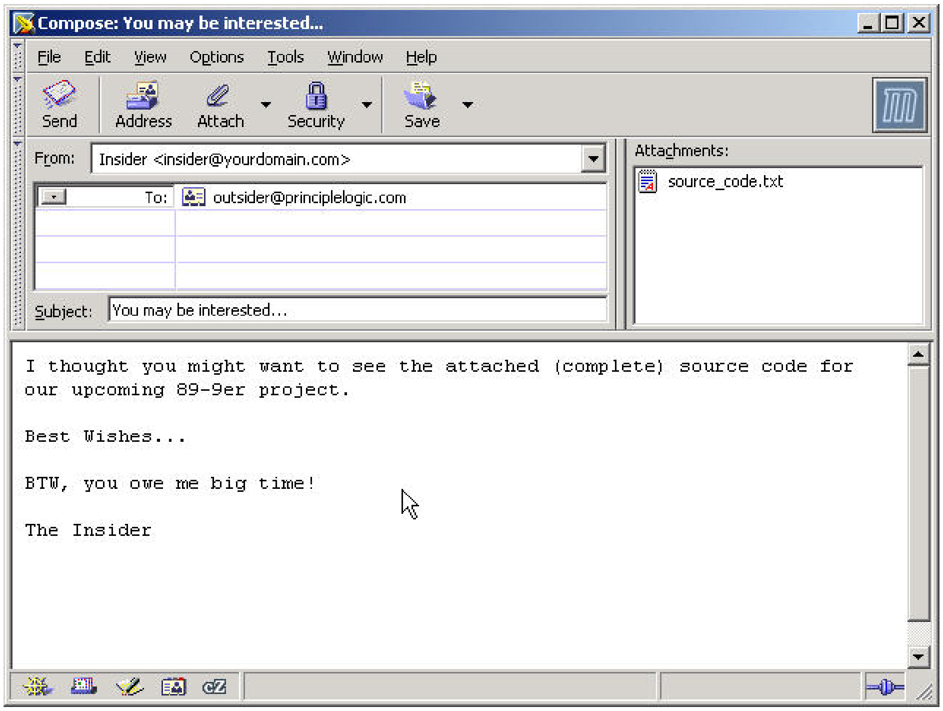
- Application service provider (ASP) services—These services offer robust content filtering (among other things such as malware and spam protection) that you don't have to manage. It's as simple as changing your DNS MX (Mail Exchanger) record to point to the ASP's server instead of your email server for all inbound email messages to be filtered. The ASP server will then forward the messages on to your server for final processing. For outbound messages, you simply configure your email server to forward messages on to the ASP server, which then processes them and forwards them on to their destinations. For those organizations that want to use the same functionality of the ASP service but would rather manage their own bandwidth and security, many ASP email security services will sell or lease you an email security appliance to host on your network; that appliance performs the same functions as the ASP's offsite server. Either way, these services allow you to offload most, if not all, of the content-filtering function, which can offer significant cost savings long term. The content-filtering services offered by ASP services are similar to those offered by server applications (see Figure 4.8).



Content Filtering:	☑ **Enable**
Character Sets:	Character Set Block: afrikaans [af] ▾ add Character Sets Blocked:
Subject Block:	add subject block ☐ Exact Match ☐ Case Sensitive ex: free mortgage loan
Subjects **blocked**:	edit / delete Free Money EM edit / delete
Message Body Text Block:	add message body text block ☐ Exact Match ☐ Case Sensitive ex: this is not spam
Message Body Text **blocked**:	edit / delete this is not spam EM edit / delete
Send Bounce:	☑ Enable
Bounce Address:	Default: *admin@mxpath.net*
Bounce Subject:	Default: *Undeliverable message returned to sender*
Bounce Text:	

Figure 4.8: Some of the filtering options offered by Singlefin's ASP content-filtering service.

- Network analyzers—A network analyzer is basically a hardware/software combination (usually run on a plain old networked PC) that captures every packet traversing the network. Network analyzers may be crude, but they can also be one of the strongest content-filtering tools. Figures 4.9 and 4.10 illustrate an email containing sensitive information as it was entered at the client along with the actual message as it was captured in transit.



From: Insider <insider@yourdomain.com>

To: outsider@principlelogic.com

Subject: You may be interested...

Attachments:
source_code.txt

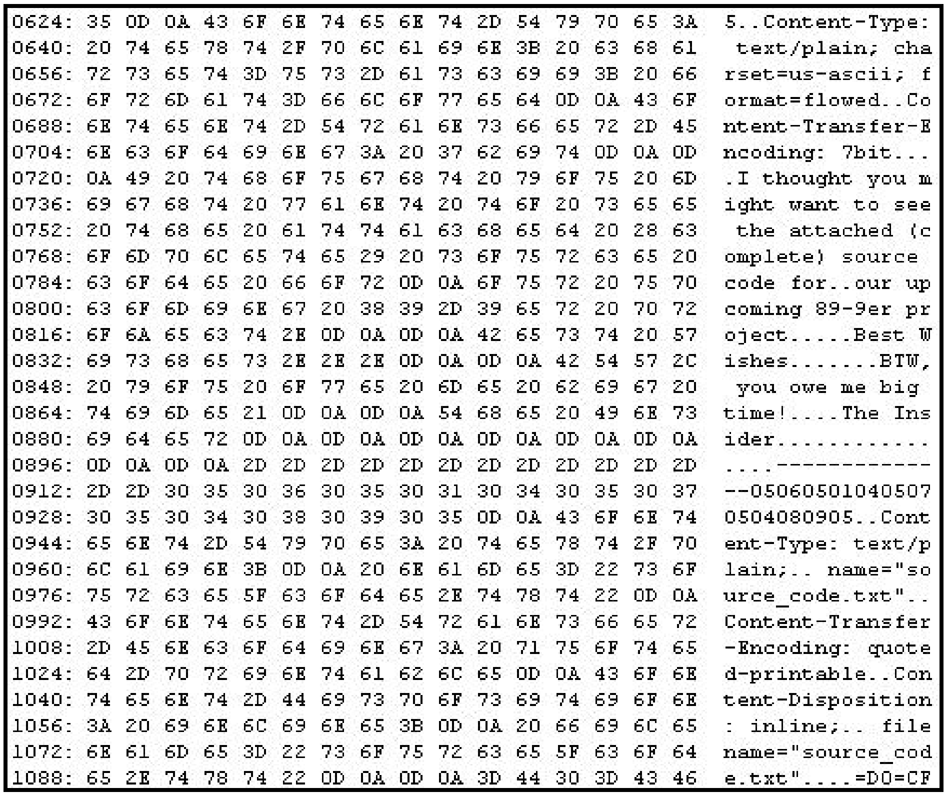
```
I thought you might want to see the attached (complete) source code for
our upcoming 89-9er project.

Best Wishes...

BTW, you owe me big time!

The Insider
```

Figure 4.9: An example of an email containing sensitive information crafted at the malicious user's desktop.



```
0624: 35 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A  5..Content-Type:
0640: 20 74 65 78 74 2F 70 6C 61 69 6E 3B 20 63 68 61   text/plain; cha
0656: 72 73 65 74 3D 75 73 2D 61 73 63 69 69 3B 20 66  rset=us-ascii; f
0672: 6F 72 6D 61 74 3D 66 6C 6F 77 65 64 0D 0A 43 6F  ormat=flowed..Co
0688: 6E 74 65 6E 74 2D 54 72 61 6E 73 66 65 72 2D 45  ntent-Transfer-E
0704: 6E 63 6F 64 69 6E 67 3A 20 37 62 69 74 0D 0A 0D  ncoding: 7bit...
0720: 0A 49 20 74 68 6F 75 67 68 74 20 79 6F 75 20 6D  .I thought you m
0736: 69 67 68 74 20 77 61 6E 74 20 74 6F 20 73 65 65  ight want to see
0752: 20 74 68 65 20 61 74 74 61 63 68 65 64 20 28 63   the attached (c
0768: 6F 6D 70 6C 65 74 65 29 20 73 6F 75 72 63 65 20  omplete) source 
0784: 63 6F 64 65 20 66 6F 72 0D 0A 6F 75 72 20 75 70  code for..our up
0800: 63 6F 6D 69 6E 67 20 38 39 2D 39 65 72 20 70 72  coming 89-9er pr
0816: 6F 6A 65 63 74 2E 0D 0A 0D 0A 42 65 73 74 20 57  oject.....Best W
0832: 69 73 68 65 73 2E 2E 2E 0D 0A 0D 0A 42 54 57 2C  ishes.......BTW,
0848: 20 79 6F 75 20 6F 77 65 20 6D 65 20 62 69 67 20   you owe me big 
0864: 74 69 6D 65 21 0D 0A 0D 0A 54 68 65 20 49 6E 73  time!....The Ins
0880: 69 64 65 72 0D 0A 0D 0A 0D 0A 0D 0A 0D 0A 0D 0A  ider............
0896: 0D 0A 0D 0A 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D  ....------------
0912: 2D 2D 30 35 30 36 30 35 30 31 30 34 30 35 30 37  --05060501040507
0928: 30 35 30 34 30 38 30 39 30 35 0D 0A 43 6F 6E 74  0504080905..Cont
0944: 65 6E 74 2D 54 79 70 65 3A 20 74 65 78 74 2F 70  ent-Type: text/p
0960: 6C 61 69 6E 3B 0D 0A 20 6E 61 6D 65 3D 22 73 6F  lain;.. name="so
0976: 75 72 63 65 5F 63 6F 64 65 2E 74 78 74 22 0D 0A  urce_code.txt"..
0992: 43 6F 6E 74 65 6E 74 2D 54 72 61 6E 73 66 65 72  Content-Transfer
1008: 2D 45 6E 63 6F 64 69 6E 67 3A 20 71 75 6F 74 65  -Encoding: quote
1024: 64 2D 70 72 69 6E 74 61 62 6C 65 0D 0A 43 6F 6E  d-printable..Con
1040: 74 65 6E 74 2D 44 69 73 70 6F 73 69 74 69 6F 6E  tent-Disposition
1056: 3A 20 69 6E 6C 69 6E 65 3B 0D 0A 20 66 69 6C 65  : inline;.. file
1072: 6E 61 6D 65 3D 22 73 6F 75 72 63 65 5F 63 6F 64  name="source_cod
1088: 65 2E 74 78 74 22 0D 0A 0D 0A 3D 44 30 3D 43 46  e.txt"....=D0=CF
```

Figure 4.10: Partial contents of this same email as captured by a network analyzer.

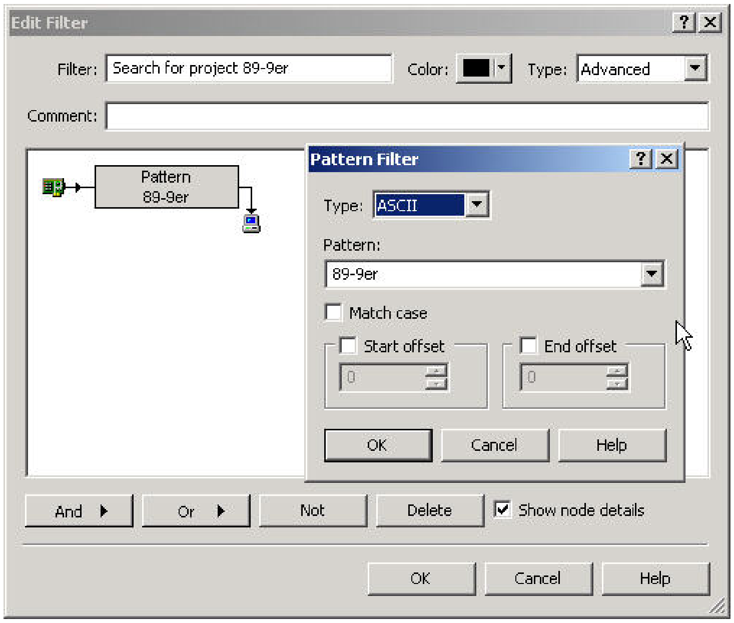
As you can see in Figure 4.10, a network analyzer shows the specific content you're looking for and then some. This level of information can be extremely valuable for content filtering as well as security incident and forensics analysis.

The main difference between network analyzers and regular content-filtering applications is that the fancy bells and whistles are missing. Network analyzer systems are autonomous—merely innocent bystanders—yet they are able to glean every possible bit of content within email messages. One benefit of this ability is the fact that they cannot be subverted other than via encryption.

> If encryption is not enabled within your email system and you are seeing encrypted SMTP traffic, this should be a red flag that something malicious is going on.

One major drawback of network analyzers is that they capture so much data that they have to be fine tuned to filter out exactly what you're looking for. In addition, only the most advanced network analyzers can block email messages or strip out sensitive information. Assuming you're running an Ethernet network, you must also run your network analyzer outside the firewall or email server on a hub-based network segment. The reason is that switched-based networks, which are common inside most networks, send packets directly between hosts instead of in a broadcast fashion within a hub environment, thus preventing the network analyzer from capturing all packets.

Figure 4.11 depicts a basic network analyzer filter that captures any traffic containing "89-9er"—the name of an upcoming product release. The great thing about network analyzers is their granularity of configuration. You can search for text strings in one protocol only (such as SMTP) or in all protocols on the network. In case you're wondering, doing so would enable you to search for information—no matter the protocol—helping to detect whether users have reconfigured their application's port number to hide their wrongdoings and to help cover their tracks.



Edit Filter

Filter: Search for project 89-9er Color: ■ Type: Advanced

Comment:

Pattern 89-9er

Pattern Filter

Type: ASCII

Pattern: 89-9er

☐ Match case

☐ Start offset 0 ☐ End offset 0

☑ Show node details

Figure 4.11: A simple EtherPeek network analyzer filter that searches for the trade secret string "89-9er" in all network traffic.

Some higher-end forensics analysis tools—which are basically intelligent network analyzers such as those provided by WildPackets, Niksun, SilentRunner, and Blue Lance—not only capture questionable network traffic but also analyze it for anomalies and allow you to replay the evidence later for further analysis. If all you need is simple email content filtering, these applications are way more than you'll ever require. In fact, while forensics analysis tools and network analyzers can provide highly technical and flexible content-filtering functionality, you're probably going to be better off with a simpler server, appliance, or ASP-based email content-filtering solution. Just know that these tools are out there in case you have the need for them at some point.

What to Look for in an Email Content Filtering Application

The following list offers specific features to look for in an email content filtering application. Keep in mind that you may not need or likely ever use all of these features. Pick the ones that you want before you shop around to make sure the products/services you're considering meet your specific requirements:

- Option to run as a dedicated application separate from your email server
- Minimal administrative requirements
- Granular controls based on user, group, time of day, computer, IP address, and so on
- Ability to remove or quarantine sensitive content or file attachments
- Offensive word lists in multiple languages
- Statistics of overall clean, modified, or blocked emails
- Preconfigured filters
- Ability to define certain events that can trigger specific actions to help enforce policies and assist with regulatory compliance
- Ability to create filters and specify keywords, start/end words in phrases, and wildcards
- Ability to differentiate upper and lower case
- Ability to quarantine or delete emails based on password protection or other anomalies
- Ability to quarantine, forward, and further analyze messages
- Ability to filter on email or attachment file size
- Ability to analyze encrypted or password-protected messages and attachments
- Ability to select specific file formats
- Ability to display warning banners
- Ability to change email header information
- Alerting capabilities
- Reporting capabilities
- Auto-generation of emails to end users (and copy administrators) who are in violation of policies

Employee Monitoring vs. Employee Privacy

You certainly won't be able to successfully implement email content filtering in your organization without addressing the issue of employee monitoring. There are specific legal issues involved with this factor.

> This section is not legal advice. Just know that, at a minimum, if your organization is going to monitor employee email usage, there needs to be a policy in place outlining all the details and your employees need to know about it.

Every company has a different reason for monitoring their employee email usage. Many organizations site productivity as their main concern. Others monitor to stay in line with governmental regulations. Regardless of the reason, there are several steps that must be taken to ensure that the organization stays in line with legal requirements and employee morale doesn't slowly fade.

> Dow Chemical fired 64 workers and disciplined 230 more in 2000 when the employees violated company policy against porn email
>
> The New York Times fired almost two dozen and disciplined another 20 employees for sending/receiving emails with sexual images and dirty jokes

Before you get started, your organization's upper management, human resources, and legal counsel must determine whether they want to passively filter email content or actively monitor employee email usage. The benefits are basically the same as those for content filtering in general—to keep the business out of hot water. The bottom line is that your organization might not be able to afford not performing some form of content filtering. There are several key issues that need attention for employee monitoring to be successful:

- Business decisions to monitor are communicated effectively to everyone
- Consistent monitoring and enforcement across the organization
- Clear policies stating what is acceptable and what is unacceptable
- Ongoing awareness training and (at least partial) employee buy-in
- Employee sign-off on policies
- Keep everyone in the loop, with no secrets or hidden agendas, to help maintain employee morale

As important as security policies and training are, they are still not as widely implemented as you might suspect (see Figure 4.12).

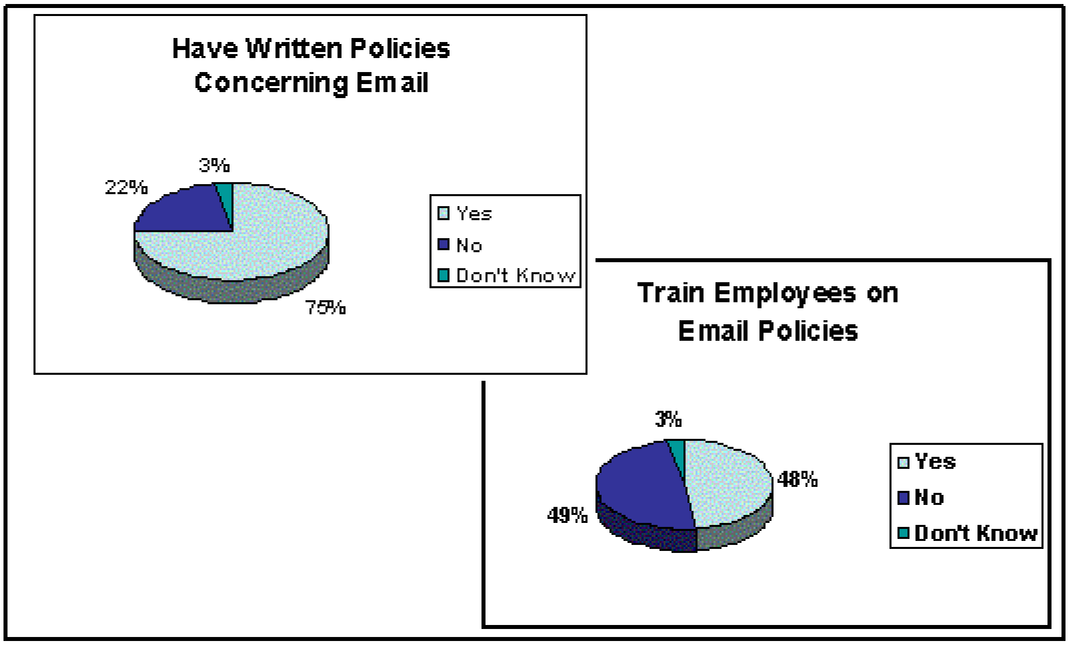


Figure 4.12: Insight into email policies in today's organizations (Source: AMA 2003 Email Rules, Policies and Practices Survey).

Content Filtering Policy Considerations

I cannot stress enough that properly designed and managed policies are the key to successful content-filtering initiatives. The process of content filtering should not be an IT-centric function. Content filtering involves serious personnel and legal issues, so it's critical that human resources, legal, and upper management be just as involved in this process. Policies must outline:

- What is being protected (email messages, and so on)
- How it is being protected (content filtering, regular monitoring, and so on)
- The business reasons why the information is being protected
- Statement that there should be no expectation of privacy when using company equipment
- Employee and other end user responsibilities in the protection process
- A statement of exactly what is acceptable and what is unacceptable to receive or send out of the organization
- How sensitive information should be handled
- If and how messages that trigger specific content-filtering rules will be quarantined or forwarded and further analyzed
- Sanctions (penalties) that will be consistently enforced after a violation has occurred
- Employee/user sign-off showing their understanding and acceptance

Be sure to check out Charles Cresson Wood's "Information Security Policies Made Easy" at http://www.netiq.com/products/pub/ispme.asp. This resource is excellent and a must-have for anyone involved with information security policy development.

SurfControl has several policy development resources on its Acceptable Use Policy Information site at http://www.surfcontrol.com/resources/aup.

If you're interested in structuring your policies in ISO 17799 format, I highly recommend you purchase a copy of it at http://www.iso.ch.

Another thing to consider regarding acceptable email usage is whether to give your employees alternatives for personal email communication. This could be as simple as requiring (and allowing) the use of Web-based or other POP3 accounts for personal use while on the company network. In addition, you could consider creating an email whitelist of addresses that are allowed for business use similar to those used in spam filtering. This could, however, end up being more administrative trouble that it's worth.

Don't forget government regulations. The following are specific U.S. Federal Government regulations that affect content filtering in some way. This list is not an exhaustive list, but rather a list of some of the more well-known sets of legislation. Use your favorite search engine to learn more about each one, and please consult with a legal expert to determine how they may affect your organization:

—Health Insurance Portability and Accountability Act (HIPAA)

—Gramm-Leach-Bliley Act (GLBA)

—Sarbanes-Oxley Act

—USA Patriot Act

—Securities and Exchange Commission (SEC) rules on electronic messaging

—Fourth Amendment of the U.S. Constitution that prohibits the monitoring of government employees

—U.S. Federal legislation that mandates a work environment free of ethnic, gender, or racial discrimination and harassment

The Future of Content Filtering

Content filtering is still in its infancy. For starters, I believe we'll see improved support for the inspection of encrypted messages. (Sounds good and scary at the same time!) This functionality is already possible but usually requires vendor-specific hardware or encryption methodologies to work properly. We will also see improved content filtering in client- and server-based email applications. At the same time, we will see more of a focus toward performing content filtering at the network perimeter and beyond in the form of hardware appliances and ASP content-filtering services in order to take the processing burden off critical email servers and keep costs to a minimum.

As in the spam-filtering world with Bayesian technology, we will see improved content-filtering capabilities to help reduce false positives. Keyword and other static rule-based filtering will become a commodity, and smarter, expert analysis will become more commonplace. In addition, there are several vendors, including Intel, that are working on embedding content-filtering capabilities in small computer chips called Application Specific Integrated Circuits (ASICs) that will improve the speed of content-filtering solutions. It will also allow us to use high end content-filtering technologies in more and more of our personal electronic devices such as PDAs and cell phones.

Watch out for Big Brother—he's here and he wants to get to know us better. As with any new technology and government initiative, there are bound to be tradeoffs between security, privacy, and personal freedoms. Government programs such as homeland security, HIPAA, and GLBA are bound to have an impact on organizational content filtering and employee monitoring in virtually every organization. These issues need to be considered in your security and privacy policy development and ongoing management initiatives. In addition, a side effect of government programs such as homeland security is that the technologies that are initially developed for these programs will eventually make their way out into the commercial marketplace.

These technologies can be good and bad from an employer and employee perspective. It will be up to you, your upper management, and your human resources and legal experts to determine how these issues fit into your overall content-filtering program. Big Brother is here to stay and we're all responsible for just how much headway he makes into our organizations and personal lives.

Content Filtering Tools and Resources

The following list provides popular content filtering solutions. However, this list is just a sampling—not a complete offering of all the content-filtering solutions available.

Vendors and Tool Providers

Blue Coat Systems at http://www.bluecoat.com

Blue Lance at http://www.bluelance.com

CipherTrust at http://www.ciphertrust.com

Clearswift at http://www.mimesweeper.com

Contexion at http://www.rulespace.com

Elron Software at http://www.elronsoftware.com

Finjan at http://www.finjan.com

Fortinet at http://www.fortinet.com

MessageLabs at http://www.messagelabs.com/home/default.asp

Mirapoint at http://www.mirapoint.com

N2H2 at http://www.n2h2.com

NETcomply at http://www.netcomply.com

Niksun at http://www.niksun.com

Ositis at http://www.ositis.com

Silent Runner at http://www.silentrunner.com

Singlefin at http://www.singlefin.net

SurfControl at http://www.surfcontrol.com

Symantec at http://www.symantec.com

Trend Micro at http://www.trendmicro.com

Vericept at http://www.vericept.com

Websense Enterprise at http://www.websense.com

WildPackets at http://www.wildpackets.com

Zixit at http://www.zixcorp.com

Resources

AMA 2003 E-Mail Rules, Policies and Practices Survey at http://www.amanet.org/research/pdfs/Email_Policies_Practices.pdf

Internet Mail Consortium at http://www.imc.org

The Extent of Systematic Monitoring of Employee E-mail and Internet Use at http://www.privacyfoundation.org/workplace/technology/extent.asp

Summary

Content filtering is an important business process that cannot be taken lightly. In this chapter, we've covered what content filtering is all about including what there is to lose if content filtering is not in place as well as what to consider filtering in your email system. We also covered how content filtering works, specific content-filtering solutions, and various employee monitoring concerns.

You've got to find a good technical and political balance when it comes to content filtering within your organization. There is no way to manually ensure that all email content is legitimate and safe—thus content filtering a great option. If you're one of the majority of organizations that is affected by some form of government regulation, the time may be here to start evaluating and implementing an email content-filtering solution. If you do choose to filter emails, just know that's only the beginning of a sometimes arduous process of investigating, disciplining, and sometimes prosecuting those involved in malicious email behavior.

As with practically any information security system, content filtering is not 100 percent foolproof. Given that, don't assume that everything is safe and secure on your email system just because you have content-filtering mechanisms in place. Email content filtering has to be an ongoing process that is properly managed. Your content-filtering rules need to be flexible and adaptable to your changing business and technical environment. Just knowing that content filtering is taking place on critical email systems, you and your upper managers can sleep better at night knowing that you're taking the right steps. That makes it worth every penny. In Chapter 5, I will cover email security in-depth including discussions about assessing email risks, email encryption, security best practices, and email security incident response.