Controlling Unwanted Content

Executive Overview

At least 50 percent of employees receive racist, sexist, pornographic, or other inappropriate email while at work.
—USA Today

Email has become an extremely powerful form of communication and data-sharing, but its reputation as a safe and secure way of collaborating is being questioned as more and more businesses are receiving inappropriate and offensive emails and attachments.

Every day more than half of all the email received by businesses is unsolicited and considered junk email or spam. Mixed in with legitimate business-related emails, are messages that are racially insensitive, include offensive jokes, divulge sensitive corporate information, and are distasteful and inappropriate. While unwanted content can pose serious productivity and legal problems, attachments can be even more threatening. Pornographic images and videos, pirated music and software, viruses, worms, Trojan horses, and other unwanted attachments can not only expose an organization to legal liability, but can also include malicious code designed to cripple entire networks. Furthermore, large attachments can devour bandwidth and seriously impact server performance and speed.

It is critical that enterprises control unwanted email content and attachments if they are to maintain the security and reliability of their networks, protect the integrity of their public image, and shield their employees and customers from offensive messages.

This white paper explains the dangers of unwanted content and attachments, and discusses the solutions available for dealing with these problems. It demonstrates that an email defense service provides the optimal layer of unwanted content and attachment control necessary for any successful corporate email security strategy.

9780 Mt. Pyramid Court, Suite 350, Denver, CO, 80112 USA
T +1.877.MXLOGIC F +1.720.895.5757 E sales@mxlogic.com
www.mxlogic.com

Email: Inherent Dangers

Email volume has been growing 40 percent annually over the past 20 years —Gartner Group.

EMAIL IS UNIVERSAL

With over 400 million corporate email boxes worldwide, no other business communications tool matches the popularity of email. From a usage perspective, email volume has been growing 40 percent annually over the past 20 years, according to a study by the *Gartner Group*. Worldwide in 2002, Internet users sent about 14.9 billion emails per day and four trillion emails per year. By 2005, this number will more than triple – to a staggering 35 billion emails a day.[1] Currently, the average employee receives 30 emails per day. These statistics alone not only demonstrate the popularity of email, but also the power it yields.

EMAIL IS EASY TO ABUSE

Because email is so easy and so instant, it can easily and instantly endanger an enterprise's network security and corporate integrity by transporting more than just business-critical communications. Email is today's superhighway being used by worm authors and spammers to on-ramp destructive viruses and bandwidth-clogging spam. According to the *Gartner Group*, anywhere from 30–50 percent or more of messages received by enterprises are malicious (viruses) or junk (spam). Furthermore, employees are also contributing to email abuse by intentionally spreading sexually- and racially-insensitive material – actions that are resulting in legal liability and corporate defamation.

BEYOND VIRUSES AND SPAM: CONTENT CONTROL

Almost all enterprises are familiar with the most common email threats: viruses and spam. And many enterprises have implemented solutions to deal with these threats. However, not all email-borne threats are viruses or spam, so email filters must also be able to detect messages that contain other types of unwanted content or attachments.

While filtering email for spam will help control unwanted content from getting inside the business email network, spam filtering and content filtering are not the same. Controlling unwanted content and attachments requires a unique and separate solution in order to be fully effective.

[1] IDC, Channel One Internet Marketing Strategy Report, March 2003

Unwanted Content: Problems

Controlling email content and attachments requires technologies above and beyond those of virus and spam filtering. Viruses are spread through executable attachments, worms are self-propagating, and spam typically travels in the form of text or HTML content. But content that can be considered offensive, sensitive, or inappropriate is often subjective, harder to differentiate from spam or viruses, and can be delivered in a variety of different formats including body copy, URLs (website addresses), and video, audio, image, or text attachments. Protecting against this variety of unwanted content requires an array of filtering techniques that take subjective preferences into account. Consider the following categories of unwanted content:

PORNOGRAPHIC MATERIAL

Although most spam is merely annoying, containing advertisements for unwanted products or services, spam can also contain offensive descriptions or images of explicit sexual acts, or offer links to websites that contain this content. Pornographic spam can be filtered with the techniques used to detect non-pornographic spam, which includes using a combination of blacklists, keyword searches, and attachment stripping programs. But this approach is usually reactive rather than proactive, meaning that it's only capable of blocking pornographic emails already recognized by anti-spam databases. Without sophisticated content filtering techniques, most pornographic images, or sexually provocative emails written by employees, can be sent undetected.

OFFENSIVE AND DEFAMATORY EMAIL

Employees often use email to share material they think is funny and amusing – the same material, however, others may find offensive, racially insensitive, or sexually harassing. If this offensive material enters just one employee's inbox, and is then passed onto others, it can soon be read by hundreds of employees or even find its way to customers, business partners, or vendors.

Unfortunately, what may seem like innocent fun can have severe consequences for an enterprise if, after receiving an off-color email, even just one of those employees feels offended or threatened enough to take legal action. Chevron Corporation was forced to pay $2.2 million to four female employees who filed a sexual harassment suit after receiving a joke via email that they considered offensive and degrading to women.

Alternatively, sending out defamatory emails has resulted in serious legal consequences for businesses. The British insurance company Norwich Union paid £450,000 in an out-of-court settlement after its staff circulated an email containing false and defamatory information about its competitor, Western Provident Association. Similarly, British Gas was forced to settle a £161,000 libel suit to rival EGS after a British Gas senior manager sent a defamatory email about EGS to 10,000 of his employees.

COMPANY-SENSITIVE INFORMATION

FBI reports indicate that most data thefts in Fortune 500 companies come from internal users.

Perhaps more damaging than the employee who transmits offensive or defamatory content is the employee who transmits sensitive information to others outside of the enterprise. Although the transmission of company-sensitive information is not always considered theft, it is often done intentionally. FBI reports indicate that most data thefts in Fortune 500 companies come from internal users and a *PC World* magazine study revealed that of 800 employees surveyed, 21-31 percent admitted to emailing sensitive or confidential material to recipients outside of their company. While the financial cost of divulging R&D secrets, confidential client information, or financial data to a competitor is incalculable, the chances of it happening are becoming more and more likely considering the ease and instantaneous nature of email.

LOSS OF BANDWIDTH

Unwanted content often comes in the form of large attachments and high-volume emails. Even if these emails are not offensive, they can significantly slow down an enterprise's email server, preventing legitimate communications from getting through. Around the holidays, office workers routinely send each other animated e-cards or videos. These large files, typically ranging in size from one to five megabytes, quickly eat up bandwidth. A situation with an employee at Chicago Bridge & Iron shows how large files can have costly ramifications. An employee with the company was stationed in Africa, where the only available Internet connection was an $8 per minute, dial-up satellite link. He was sent a six-megabyte file that would have taken 75 minutes to

download – at a total connection cost of $600. Fortunately, this attachment was blocked before it was transmitted, and the connection cost was saved. While large files and attachments may not always be offensive or proprietary, they consume bandwidth, and bandwidth costs money. The more an enterprise can control the volume and size of traffic into and out of its network, the more it can control bandwidth costs.

PIRATED MUSIC AND SOFTWARE

The proliferation of pirated music and software files (as well as the increasing popularity of pirated movies) available on the Internet means an increase in potential liability for corporations if their employees traffic this material while using their company's network. The Business Software Alliance has recovered more than $60 million over the past 10 years from corporations caught with pirated, or unlicensed, software. And the ongoing legal battles over peer-to-peer file sharing, which traffics the vast majority of pirated music and video files, looks as if it will be won by the entertainment industry. They are seeking extreme copyright protection, including the ability to sue any and all parties involved in the process of transmitting pirated files. In fact, a corporation can be liable for hundreds or even thousands of dollars per song file found on its network.

Unwanted Content: Solutions

Just as methods exist for controlling viruses and spam, there are a number of available solutions for controlling unwanted content. These solutions range from simply blocking unwanted attachments based on size or type, to the more complex techniques that use heuristic and statistical scanning to identify unwanted content in context.

A recent survey by Osterman Research indicates that only 32 percent of enterprises filter email for unwanted content other than spam. However, much unwanted content (offensive material and images, company-sensitive information, large attachments, pirated music, etc.) is not spam. That means almost 70 percent of enterprises are unable to control the content of emails entering and leaving their network. With the right solutions, however, controlling email content is possible. These solutions include:

KEYWORD FILTERING

Perhaps the most effective way to filter email for unwanted content is to scan messages for keywords. These can be anything from offensive, profane, and pornographic terms, to words or phrases that represent company-sensitive information, like "Project XYZ," or "Company ABC Projected Earnings." Usually content filtering technologies come pre-configured with lists of standard keywords – offensive material, pornography, and profanity. More sophisticated solutions allow an enterprise to add its own keywords, so email flowing into and out of its network can be scanned for company-specific content.

ATTACHMENT CONTROL

Only 40 percent of companies have deployed systems aimed at filtering email for pornography. — Osterman Research

Attachment control is necessary to both prevent unwanted and illegal content and to reduce bandwidth congestion. A good content control solution allows an enterprise to select the types and size of attachments to block. According to Osterman Research, 75 percent of enterprises block one or more types of email attachments, and 51 percent of enterprises block email messages that exceed a certain size. At a minimum, good email filters should have the capacity to block attachments containing certain unwanted file types, and messages or attachments that exceed a given size.

MANAGED CONTENT CONTROL SOLUTIONS

An enterprise must utilize all of the above techniques for the best protection against unwanted content. However, gathering and implementing these solutions separately can be expensive and time-consuming. Increasingly, enterprises are looking for solutions that provide many content control techniques in one bundled service. But most bundled services still require in-house installation, integration and maintenance, necessitating increased hardware, software, and IT resources.

For this reason, managed content control solutions are being utilized by organizations intent on adding protection without dealing with the hassle and expense of providing that protection in-house. MX Logic's Content and Attachment Filtering, part of its comprehensive email defense solution, is ideal for enterprises of any size.

9780 Mt. Pyramid Court, Suite 350, Denver, CO, 80112 USA
T +1.877.MXLOGIC F +1.720.895.5757 E sales@mxlogic.com
www.mxlogic.com

MX Logic: Content and Attachment Filtering

In addition to Spam Blocking, which can help to provide a first layer of email content control, Content and Attachment Filtering, a component of MX Logic's Email Defense Service, provides comprehensive filtering for unwanted content, including critical keyword filtering and attachment control.

CONTENT AND ATTACHMENT FILTERING: KEYWORD FILTERING

Content and Attachment Filtering evaluates the content of all messages based on the policies and associated actions configured by the organization. These policies can be quickly and easily configured to disallow the inbound and outbound transmission of private or proprietary corporate data, racially- and sexually-insensitive material, profanity, and other content deemed inappropriate by the enterprise.

Content and Attachment Filtering uses a "bucket" configuration to organize keywords. These buckets ("Profanity," "Sexual Overtones," "Racially Insensitive," etc.) contain related keywords which, when detected, indicate that the message contains unwanted content. Each bucket can be turned on and off, depending on the organization's policies. Additionally, Content and Attachment Filtering allows an enterprise to create its own keyword bucket, so it can filter messages for sensitive corporate information, as well as any words or phrases that the enterprise would like to use to prevent specific content from entering or leaving its network.

CONTENT AND ATTACHMENT FILTERING: ATTACHMENT CONTROL

Content and Attachment Filtering blocks unwanted attachments before they enter or exit the corporate network. Attachments are filtered according to configurations set by the enterprise IT administrator. Attachments can be filtered in a number of ways: by size, by MIME media type (.exe, .vbs, .mp3, etc.), by binary content (making sure the attachment's content matches the indicated file type), and, if they are images, by image analysis.

Summary

Controlling the content of email that enters and leaves an enterprise network requires more than simply blocking spam and viruses. It requires a combination of solutions, including keyword filtering and attachment control. But because controlling content and other email

threats is expensive and time-consuming, more and more enterprises are shifting this burden to managed email defense services. These organizations understand that filtering email before it enters their network provides them with a highly effective primary layer of security at a lower cost than providing the same set of services in-house.

Controlling content is a serious problem for any competitive enterprise. And while solutions exist to help solve the problem, the best solution filters unwanted content before it enters the enterprise network, and catches it before it reaches external recipients. Content and Attachment Filtering, part of MX Logic's Email Defense Service, meets all of these requirements and provides the most complete content control solution available for the corporate enterprise.

About MX Logic

MX Logic, Inc. provides innovative email defense solutions that ensure email protection and security for enterprises, service providers, government organizations, and resellers and their customers. Deployed as a managed service or on-premise software, the company's feature-rich solution suite is the industry's most comprehensive, flexible and easy to use.

MX Logic's cost-effective service provides around-the-clock email protection, automatically intercepting, analyzing and blocking malicious and unsolicited messages at the network perimeter—before they can enter or leave an internal network. Unlike other email protection solutions, MX Logic's services act as a "proxy," filtering messages in-line as they are delivered to the customer – reducing the risk of message loss common to the store-and-forward method used by other providers. Using a patent-pending Stacked Classification Framework®, which leverages the strengths of five spam-fighting filters, MX Logic can accurately stop 98 percent of spam and viruses at the network perimeter. Fortifying the filtering process with two industry-leading anti-virus engines makes our Email Defense Service one of the most comprehensive solutions on the market today.

Through the company's managed service offering, MX Logic processes millions of messages per day for over 2,500 organizations, including EnCana, Hyundai Motor America, The Sports Authority, YMCA, and ServiceMaster. In addition, MX Logic is the only email defense company to offer both a managed service and a turnkey, carrier-grade software solution for service providers. For more information, visit www.mxlogic.com.

9780 Mt. Pyramid Court, Suite 350, Denver, CO, 80112 USA
T +1.877.MXLOGIC F +1.720.895.5757 E sales@mxlogic.com
www.mxlogic.com