

Messaging Threats in the Enterprise



an Osterman Research white paper

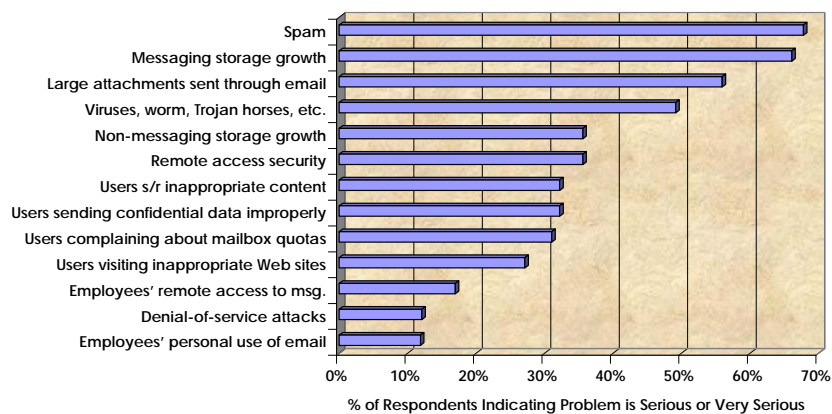
Messaging Systems Are Under Siege

As any messaging administrator can confirm, threats to messaging are, at best, a headache and, at worst, capable of causing significant harm to an enterprise. Spam is clearly the most critical problem facing messaging and network administrators today and the problem is getting worse: spam has grown from a minor annoyance less than two years ago, representing less than 20% of all email traffic at that time, to a major problem today, representing well over 50% of all email. For some enterprises, the situation is even more dire: for example, a major healthcare company in the United States currently experiences an inbound spam rate of 83%.

Spam is clearly the most critical problem facing messaging and network administrators today.

In an Osterman Research survey conducted for BorderWare Technologies, spam was identified as the most serious problem facing messaging managers today: 68% of organizations identified spam as a "serious" or "very serious" problem, as shown in the following figure.

Leading IT-Related Problems in the Enterprise
(% of Respondents Indicating Problem is Serious or Very Serious)



In addition to spam, messaging storage growth, large attachments and viruses/worms and related threats were also identified as critical problems currently facing enterprise IT administrators.

Why are These Problems Getting Worse?

Spam is getting worse due to a number of factors, but these are the key factors that are making the problem so serious:

- More individuals and companies are now using spam as a sales and marketing technique because it is an

extremely inexpensive, albeit inefficient, method for delivering a message to prospective customers.

- A sufficient number of recipients of these messages respond to them so as to make the practice of sending spam sufficiently worthwhile for spammers to continue.
- Spammers are becoming increasingly sophisticated in their efforts to bypass spam filtering technologies. Many of these technologies are earlier generation approaches, such as real-time blacklists, that are not effective at dealing with the spam problem.

One source estimates that one-third of email server processing is devoted simply to processing Directory Harvest Attacks.

Another problem related to spam is the Directory (or Dictionary) Harvest Attack (DHA). In a DHA, an automated system will send thousands of messages to a server, each message using a slight variation of an email address. Because an unprotected email server will dutifully respond when an email address is not valid, spammers can quickly and automatically add non-bounced messages to a list of valid email addresses. One source estimates that one-third of email server processing is devoted simply to processing DHAs.

Messaging storage growth and the increasing use of attachments are also serious problems, as noted above. A recent Osterman Research survey found that messaging storage requirements grew nearly 40% between mid-2002 and mid-2003. This growth has been caused by increasing use of messaging in general, but also by the increasing use of attachments, particularly large attachments, such as Microsoft PowerPoint files, images, MP3 files and the like. Increased messaging storage adds to the labor cost of managing a messaging system, it requires more hardware to store the ever expanding content, it lengthens server restoration times and also complicates the archiving of older messaging system content.

Viruses, worms, Trojan horses and related problems continue to be a problem, flaring up into very serious threats for many enterprises.

Viruses, worms, Trojan horses and related problems continue to be a problem, flaring up into very serious threats for many enterprises, as evidenced by this summer's outbreak of the Blaster worm, the Sobig.F virus and other malicious code. The problems associated with these threats range from minor annoyances and loss of productivity to destruction of data and potentially more serious problems. The serious impact of malicious code is due in large part to two factors: the difficulty associated with keeping messaging defenses current, coupled with the large number of entry points for

these threats. For example, in the BorderWare survey it was discovered that 25% of all enterprise users access either the corporate messaging system or network remotely. Making the corporate messaging system and network accessible for remote users and simultaneously keeping it secure simply add to the problems faced by messaging administrators.

The Problems Caused by Spam and Other Messaging Threats

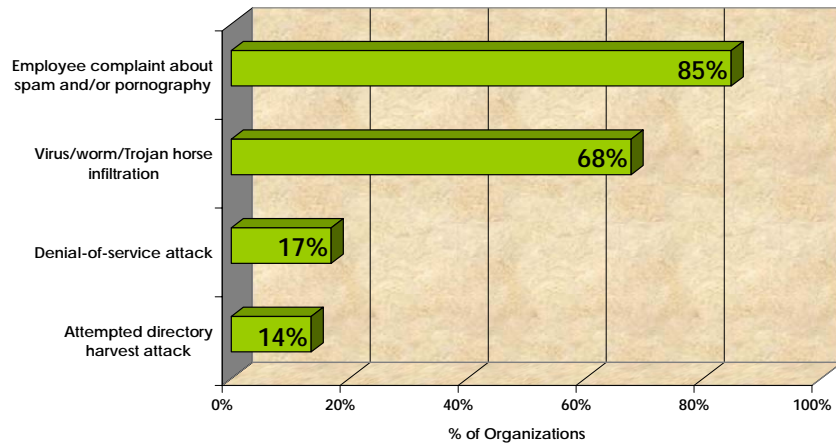
Spam, the most serious problem facing enterprise messaging managers, causes a variety of problems for the typical enterprise:

An end user that is not protected by spam blocking technology costs an organization \$1,400 each year in lost productivity simply because he or she must deal with the spam that enters his or her mailbox.

- **Spam consumes critical IT resources and increases the cost of email.** In addition to increased storage requirements, spam also reduces server performance, consumes network bandwidth, slows message delivery times, increases email server downtime and increases the amount of administrative labor required to manage the email system.
- **Spam reduces the productivity of employees who are forced to deal with the flood of unwanted messages delivered to their mailboxes.** An end user that is not protected by spam blocking technology costs an organization \$1,400 each year in lost productivity simply because he or she must deal with the spam that enters his or her mailbox. Also, these productivity losses do not take into account the productivity loss from employees who read spam messages or buy products advertised in them. For example, our research found that the typical employee responds to more than seven messages each month.
- **Spam is becoming a more serious issue from a legal perspective.** Because a growing percentage of spam is pornographic or otherwise offensive in nature, enterprises will be liable for significant damages if they do not at least attempt to prevent delivery of this content to their end users either through the creation of corporate policies and/or the deployment of spam-blocking technology.

As shown in the following figure, employee complaints about spam and/or pornography are more common than the infiltration of viruses, worms or Trojan horses – in 85% of enterprises surveyed, there had been an employee complaint about spam and/or pornography during the previous 30 days.

Enterprise Messaging Problems That Have Occurred in the Enterprise During the Past Month



Pornographic and other offensive content delivered via email will become a more serious problem for the enterprise in the coming months.

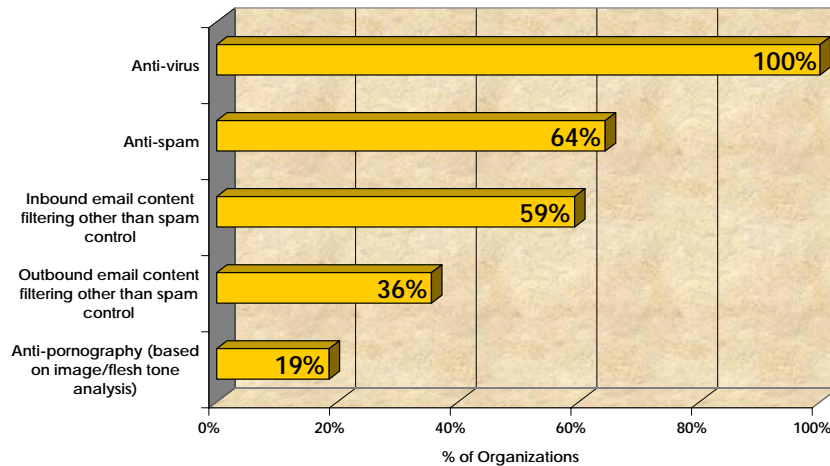
As noted above, pornographic and other offensive content delivered via email will become a more serious problem for the enterprise in the coming months. Osterman Research anticipates that pornography-related issues will supercede spam as one of the key problems for the enterprise during 2004. The problems that can arise from pornography delivered via email – whether this is from an external source or delivered from one employee to another – center on ‘hostile workplace’ issues and the potential liability that employers face if they do not protect their employees from this content. A number of legal actions have already been brought by plaintiffs specifically related to their receipt of offensive email and the number of such cases is expected to increase.

What Enterprises Are Doing in Response

To thwart messaging-related threats, virtually all enterprises have deployed anti-virus systems, and most have also deployed some sort of spam-blocking and inbound content filtering systems. However, only about one-third of enterprises have deployed any sort of outbound content filtering system, and only one in five enterprises has deployed a pornography-blocking system, as shown in the following figure.

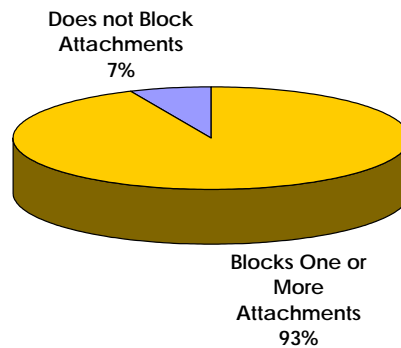
One of the most common methods for reducing the impact of messaging-related threats is to block attachments of various types.

Deployment of Messaging Threat Tools in the Enterprise



In addition to the deployment of the messaging defense systems noted above, one of the most common methods for reducing the impact of messaging-related threats is to block attachments of various types. As shown in the following figure, more than 90% of enterprises currently block one or more attachment types in their messaging system.

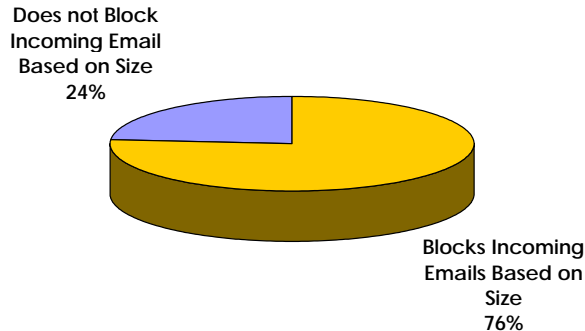
Current State of Attachment Blocking in the Enterprise



Although not as common as blocking attachments by type, blocking attachments based on their size is the norm in many enterprises, often to reduce network bandwidth requirements. As shown in the following figure, three in four enterprises currently blocks attachments above a certain size.

Current State of Blocking Incoming Email Based on Size

A key problem with blocking attachments by type or based on their size is that a significant number of valid messages and attachments simply do not get through to recipients.

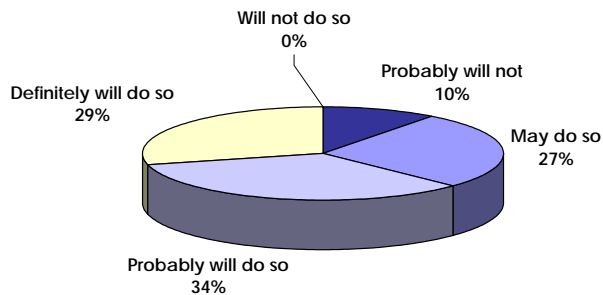


A key problem with blocking attachments by type or based on their size is that a significant number of valid messages and attachments simply do not get through to recipients. This creates an additional problem related to the “false positive” issue associated with spam-blocking systems, because it prevents otherwise valid content from reaching end users. The problems associated with blocking this content can range from a loss of user productivity when email recipients must track down the cause of not receiving a message, to serious financial consequences from not receiving an important email.

Messaging is in a State of Flux

The myriad threats to messaging – spam, viruses, pornography and other problems – are causing many enterprises to reassess their current email defense infrastructure. As shown in the following chart, nearly two-thirds of enterprises will probably or definitely reassess how they handle messaging-related threats at some point during the next 12 months.

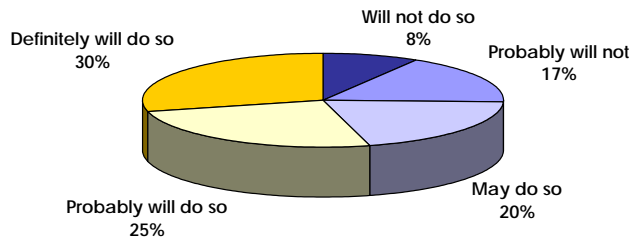
Likelihood of Reassessing the Email Defense Infrastructure During the Next 12 Months



Reassessing either the entire email defense infrastructure – or the entire email infrastructure itself – are extremely expensive and difficult options for enterprises to consider.

An even more difficult – and more expensive – option that will be undertaken by many enterprises will be to reassess the entire email infrastructure, which is being driven, at least in part, by messaging-related threats. As shown in the following figure, more than one-half of enterprises will probably or definitely undertake such a reassessment by the end of 2004.

Likelihood Reassessing the Entire Email Infrastructure During the Next 12 Months



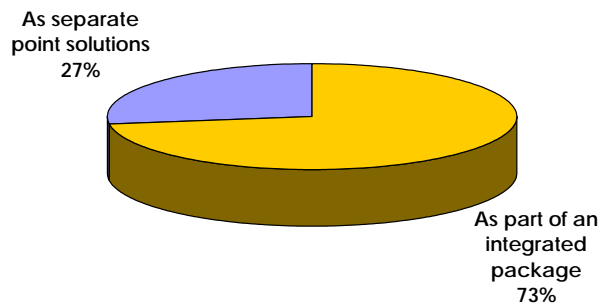
Reassessing either the entire email defense infrastructure – or the entire email infrastructure itself – are extremely expensive and difficult options for enterprises to consider. However, the severity of the problems associated with messaging threats and other messaging-related problems is driving many enterprises to at least consider going through the reassessment process in order to make email secure and reliable, and to reduce the liability associated with these threats.

What Enterprises Need To Do

Clearly, enterprises need a way to manage their messaging systems efficiently and to prevent threats from negatively impacting either the messaging or network infrastructure. Most enterprises would prefer messaging-threat solutions integrated into a single package that will deal with spam, viruses, pornography and other threats to the messaging system. As shown in the following figure, nearly three out of four enterprises would prefer such an integrated offering over separate point solutions that deal with specific messaging-related threats.

Most enterprises would prefer messaging-threat solutions integrated into a single package that will deal with spam, viruses, pornography and other threats to the messaging system.

Preference for Purchasing Messaging Threat Solutions



BorderWare's Offerings

One vendor that provides an integrated security offering that addresses the key threats to a messaging system on multiple levels is BorderWare Technologies Inc.

The company makes a series of "application-specific" appliances for network firewall+VPN, email, DNS, and document collaboration, that are deployed at various military, intelligence, defense and national security agencies, and corporations worldwide. Founded in 1994, BorderWare is a private company headquartered in Toronto, Canada with sales offices in: London; Frankfurt; Stockholm; Dallas, Texas; Washington DC; and San Jose, California.

For email, BorderWare offers the MXtreme Mail Firewall appliance. A third generation product, MXtreme is an easily deployed firewall product that sits between enterprise messaging servers and the Internet, protecting mail systems from all threats including spam, viruses, Trojans and worms, to malformed messages and denial-of-service attacks, while enabling overall email server functionality, sophisticated routing and delivery, and secure remote access.

MXtreme features:

- Spam-blocking that uses a variety of techniques to identify and block spam, including configurable filters, smart pattern matching to identify suspicious messages and realtime blacklists. In addition, MXtreme integrates the Brightmail Anti-Spam Enterprise Edition, providing Brightmail's managed anti-spam service as a cost option that requires zero customer IT administration.
- Virus scanning using Kaspersky Labs, which is an unlimited license included with the product at no additional cost.
- Secure Webmail that allows full, secure access to internal mail servers. Users can access their mailboxes using Microsoft Outlook Web Access, Lotus iNotes or BorderWare's internally developed Webmail client.
- Content filtering (both inbound and outbound) that can protect an enterprise from offensive content, leaks of confidential data and other threats.

The MXtreme Mail Firewall appliance is an easily deployed firewall product that sits between enterprise messaging servers and the Internet.

- Encryption using SSL/TLS that allows all inbound and outbound email content to be encrypted, including connections to remote systems.
- Identification of malformed data packets and malformed messages that can allow viruses to impact messaging servers.
- Full remote and local management capability through a simple, Web-based interface, including the ability to encrypt data for additional security. MXtreme advanced reporting capabilities also enable proactive capacity planning to help messaging managers better plan their messaging capacity.

The MXtreme Mail Firewall appliance also provides other features and capabilities, including configurable mail delivery and an automated update service. In addition, MXtreme can also host mailboxes, acting as a messaging server, which is particularly advantageous for small offices that might operate as satellite locations to a corporate headquarters.

The Benefits of MXtreme

Deploying MXtreme to protect an enterprise's email infrastructure delivers a number of benefits:

- Lower IT administration costs
 - A "Plug, Play, Forget" appliance that installs in minutes
 - Built upon S-Core, a hardened OS that is Common Criteria EAL 4+ Certified and self-updates (through SecurityConnection feature)
 - Zero administration spam filtering with Brightmail
 - Real-time anti-virus updates with Kaspersky
- Increased Quality of Service
 - Email always available for users and customers
 - Dedicated hardware increases throughput
 - Ability to deploy in parallel with firewall for bandwidth improvements
 - Increased user productivity (both internal and remote users)
 - No time wasted on spam, viruses, worms, etc. at the user level
 - Fronts Outlook Web Access and iNotes for secure remote access

- Reduced Security Risks
 - Kaspersky AntiVirus at the perimeter adds to defense-in-depth strategy
 - MXtreme is "invisible" and impervious to port scanning
 - Inbound/Outbound content filtering ensures confidential material remains confidential
 - Encryption for sensitive information

The MXtreme Mail Firewall appliance is available in three different models based on the messaging traffic requirements of an organization.

For more information, please visit www.borderware.com.

© 2003 Osterman Research, Inc. All rights reserved.

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

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