



Messaging Security Market Trends, 2006-2009

Report Focus

Messaging security is among the most critical elements of any organization's IT initiatives. Because of the growth in the variety and severity of threats, including viruses, worms, spam, phishing attacks, spyware denial-of-service attacks and other threats; and because of messaging's central role in the operation of virtually an organization; maintaining adequate security for messaging capabilities is critical and will be increasingly so during the coming years.

This report is focused on messaging security issues in North American organizations and discusses the results of three separate surveys that were focused on messaging security and related issues in mid-sized and large organizations.

Key Findings and Trends Discussed in this Report

- Eighty-four percent of organizations have had a virus, worm or Trojan horse successfully infiltrate their network through email, while 54% of organizations have had such a threat successfully enter their network through the Web. However, only about one in five organizations have been infected by a public instant messaging (IM) network worm or virus.
- The most serious messaging and security problems faced by organizations include growth in email storage requirements, inadequate email archiving, employees sending confidential data via email or IM and employees sending and receiving inappropriate content.
- Most organizations have moved beyond first-generation anti-virus and anti-spam capabilities, replacing these in favor of more effective solutions. However, among organizations that are using more sophisticated capabilities for outbound email content filtering or email encryption, for example, first-generation systems are still the primary tools in use.
- The perceived legitimacy of different communications applications employed in the workplace varies widely. While 96% of organizations view Web conferencing as a legitimate application in the context of business communication, only 42% view consumer Webmail as legitimate, while even fewer view tools like peer-to-peer (P2P) file-sharing systems or Skype as legitimate.
- Although many organizations have deployed an enterprise-grade IM solution, most have not yet done so. Approximately two-thirds of organizations indicate that they have plans to deploy an enterprise-grade IM solution by Q2/2007.



- When asked about spam-blocking efficiency over time, 39% of decision-makers felt their systems provided consistent performance, 37% said that spam-block efficiency is improving, while 24% of respondents indicated that the problem is getting worse. When asked about the efficiency of anti-spam software with regard to its ability not to generate a false positive, 51% indicated that things are staying about the same, while 35% said that things are getting better. Only 14% of respondents said that the problem is getting worse.
- While 73% of organizations use a series of point, best-of-breed solutions for email security, only 33% actually prefer this approach. By contrast, while 27% of organizations use an integrated messaging security product with a single administrative interface, nearly one-half of organizations would prefer to do so.
- Organizations are planning to make substantial investments in messaging systems during the next year. During the 2006-2007 period, nearly three-quarters of organizations plan to make investments in their enterprise email systems, two-thirds of organizations plan investments in adware/spyware protection and more than one-half of organizations plan to invest in Web conferencing or other online collaboration systems.

Table of Contents

1. Executive Summary	1
2. Methodology and Overview	9
3. Current Messaging Security Practices and Problems.....	11
4. Anti-Spam and Anti-Virus.....	21
5. Encrypted Messaging	27
6. Content Filtering and Compliance	41
7. Instant Messaging Security.....	49
8. Other Security Issues	55
9. Preferences for Security Delivery Models	65
10. Security Investments and Budget Issues	75
11. Vendors of Messaging Security Solutions.....	79



List of Figures

Messaging Systems in Use Based on the Percentage of Users Who Employ Each as their Primary Email System	9
Email- and Web-Related Security Problems Experienced by Organizations	11
Penetration of Various Communications Technologies, 2006-2007	14
Penetration of Wireless Handhelds Accessing Email, 2006-2007	17
Perceived Legitimacy of Various Applications	18
Perceived Importance of Providing Hygiene, Content Inspection and Logging/Forensics for Legitimate Applications	19
Changes in Spam-Blocking Efficiency over Time	21
Changes in Spam False Positive Efficiency over Time	22
Perceived Importance of Zero-Hour Virus Protection	24
Views on the Integration of Zero-Hour Virus Protection with Anti-Virus Systems	24
Sources that Organizations Would Consider When Procuring Zero-Hour Virus Protection	25
Organizations' Plans for Email Encryption	27
Devices/Systems in Which Email Encryption Will Be Used	28
Groups to Which Encrypted Messaging Would be Deployed	30
Leading Drivers for Encrypted Messaging	31
Organizations' Reasons for Not Using Encrypted Messaging	32
Importance of Various Characteristics for Email Encryption Solutions	33
Importance of Various Factors in Justifying Email Encryption to Non-IT Senior Management	34
Types of Communication Traffic for Which It Is Important to Have a Messaging Encryption Solution	35
Encryption Methods That Organizations Need to Communicate Securely	36
Preferences for a Gateway-Based Email Encryption Solution	36
Departments and Business Groups That Would Have Funding for Messaging Encryption Solutions	37
Departments and Business Groups That Would Implement and Manage Messaging Encryption Solutions	38
North American Market for Encrypted Email, 2006-2009	39
"Does your organization require email messages to be reviewed and approved by others before being sent outside the organization?"	41
Demand for Organization-Specific Compliance Policies	42
Corporate or Regulatory Policies That Organizations Would Want to Enforce With a Content Filtering Solution	44
Level of Concern About the Leakage of Sensitive Information Via Approved and Supported Communications Channels	45
Communications Applications/Protocols That Require Content Filtering for Compliance	46



List of Figures (concluded)

Preferences for Delivery of Outbound Compliance Monitoring Capabilities	47
“Has your user base ever been impacted or infected by a public IM network worm or virus?”	49
Tools and Capabilities Used to Limit or Block Unwanted IM Use.....	51
Organizations' Plans for Deploying an IM Management and Security Solution.....	51
Status of Organizations' Deployment of Enterprise-Grade IM Solutions.....	52
Organizations' Plans for Deploying an Enterprise-Grade IM Solution	53
The Impact of Security as a Consideration in Deciding to Deploy an Enterprise-Grade IM Solution	53
Compliance Requirements to Which Organizations Perceive Instant Messages are Subject.....	54
Organizations' Views on Adware/Spyware.....	55
Organizations' Current Approaches to Limiting Adware/Spyware	56
Organizations' Level of Concern Over Managing External (Public) Webmail	57
Organizations' Views on Dealing with Webmail-Related Threats	58
Status of Outbound Filtering Capability Deployment	58
Organizations' Reasons for Deploying a URL Filtering Solution	59
Organizations' Reasons for Deploying an Intrusion-Protection Solution.....	60
Capabilities Used to Limit or Block Unwanted Peer-to-Peer File-Sharing Use	61
Methods Used to Send and Receive Large Files	62
Organizations' Concerns That Current File Transfer Solutions Might Not Be Compliant	63
Organizations' Views on the Desirability of Various Delivery Models for Email Security	65
Current Practices vs. Preferences for Delivering Email Security Capabilities	66
Current Practices vs. Preferences for Delivering Desktop Security, Web Security and Intrusion Prevention	67
Organizations' Likelihood of Evaluating an MSP for Email Security.....	68
Organizations' Likelihood of Using an MSP for Email Security	69
Vendors That Organizations Would Consider for Managed Service Provision.....	70
Organizations' Views on MSP Attributes.....	71
Desirability of Various Deployment Options for IM Management.....	72
Forecast of Hosted Messaging Security Penetration, 2006-2009	73
Focus of Organizational Investment in Messaging Technologies, 2006-2007	75
Messaging Technologies for Which Organizations Currently or Will Have Budget, 2006-2007	76
Organizational Expenditures on Email Security per User	77
Email and IM Security Budgets per User, 2005-2006	78



List of Tables

Messaging and Security Problems That Organizations Rate as Serious or Very Serious	12
Deployment and Location of Various Messaging Security Capabilities, Mid-2006.....	15
Deployment and Location of Various Messaging Security Capabilities, Late 2007.....	15
Generation of Messaging Security System in Place Among Organizations That Have Security Capabilities.....	16
Penetration of Email Encryption into Various Groups	29
Penetration of Email Encryption into Various Parts of Organizations	30
Non-Email Encryption Capabilities in Place and Planned.....	32
Importance of Various IM Management Features	50
Agreement with Various Statements About Messaging Policy Management	63
Agreement with Various Statements About Messaging Security Capabilities	70
Likelihood of Using Various Messaging Security Vendors.....	79
Vendors of Email and IM Security Products and Services.....	80

About Osterman Research, Inc.

Osterman Research, Inc. provides market research, cost modeling, benchmarking and related services to vendors of technology-based products and services.

We help vendors, IT departments and other organizations make better decisions through the acquisition and application of relevant, accurate and timely data on markets, market trends, products and technologies. We also help vendors of technology-oriented products and services to understand the needs of their current and prospective customers.

Part of what makes us unique is our market research panel: a large and growing group of IT professionals and end-users around the world with whom we conduct our research surveys. This allows us to conduct surveys quickly and accurately.



Messaging Security Market Trends, 2006-2009
was published in July 2006 and is available for \$2,195



For more information on Osterman Research,
or if you have any questions about this
report, please contact us at:

Osterman Research, Inc.

P.O. Box 1058
Black Diamond, WA 98010-1058

Tel: +1 253 630 5839

Fax: +1 866 842 3274

Email: info@ostermanresearch.com

<http://www.ostermanresearch.com>



Order Form

Messaging Security Market Trends, 2006-2009

Available NOW for \$2,195

*Includes hard copy and electronic copy of report,
as well as electronic copy of all survey data. All materials
can be used throughout your organization.*

*This report can also be ordered online at
<http://www.ostermanresearch.com/orderform.htm>*

BILLING INFORMATION	
Name	Telephone
Organization	Fax
Street Address	Email
City, State, Zip/Postal Code	Country
SHIPPING INFORMATION <i>(if same as above, please leave blank)</i>	
Name	Telephone
Organization	Fax
Street Address	Email
City, State, Zip/Postal Code	Country
Method of Payment	
<input type="checkbox"/> Visa	Credit card #: _____
<input type="checkbox"/> MasterCard	Exp. date (MM/YY): ____ / ____
<input type="checkbox"/> Please send invoice	Purchase order #: _____
<input type="checkbox"/> Payment is enclosed	
<input type="checkbox"/> Please contact me to arrange payment	
Please note requested billing arrangements:	