

# Managing Business Messaging

The Executive Guide to Integrated Message Management: Security, Availability, Compliance and Visibility



## Email and Instant Messaging – Just what are the Threats?

The whole corporate communications landscape is changing rapidly, not only in terms of steadily increasing volumes of emails, but also in terms of the complexity, variety and speed of attacks.

**Email** is now an essential corporate communications tool, but corporate IT departments now face urgent challenges in securing and managing other aspects of their messaging systems. It is no longer simply a matter of blocking malicious and unwanted messages; managing legitimate electronic correspondence is now of paramount importance.

New threats carried by **Instant Messaging (IM)**; ensuring the availability of messaging service; and new **Governance & Compliance** requirements demanding that companies sanitize and retain relevant messages, are in the forefront of messaging issues today.



Viruses, worms, hacks and other security threats have increased more than 22% during 2005

PricewaterhouseCoopers study,  
Computing October 2005

### Email threats

Email threats include spam, viruses and trojans as well as directory harvesting, phishing and zombie attacks.

- Spam now represents 60-80% of all email communication
- Spam introduces offensive and undesirable content
- The costs of spam are measured in lost productivity, and additional infrastructure needed to manage an ever-increasing number of messages
- Viruses, trojans and other malware are fairly well understood but continue to absorb IT resources in combating them
- Directory harvesting is a relatively new and insidious 'dictionary' type attack, which aims to collect all email addresses within an organization
- Phishing is a key tactic in identity fraud, and continues to pose real threats, especially to the individual
- Zombie attacks install malware on the victim's PC, enabling spammers to take control of the PC, network it with thousands of other zombies, and send out millions of spam emails, or launch DoS (denial of service) attacks – or use it for any other purpose they desire...



Whereas a hacker might take months or years to try to crack a highly secure system through sheer persistence, Beechey says an internet worm can breach defenses in seconds

Paul Beechey of QinetiQ,  
Computing October 2005

### Instant Messaging Threats

#### **IM (e.g. Yahoo! AOL and MSN) create significant problems:**

Users have typically installed the software themselves leaving IT professionals with no control over IM, little or no supervisory capabilities, and no standards, identity management or security procedures in place to control its use.

**IM worms** spread very rapidly compared to other threats such as email viruses. A comparison of three recent virus types by IMlogic reveals that IM worms have vastly compressed the time available to respond to these threats.

- Code Red, a TCP/IP borne worm took 14 hours to infect 500,000 hosts
- The Slammer virus, an email worm, infected 500,000 hosts in 20 minutes
- IM worms can infect 500,000 hosts in an astounding 30 to 40 seconds!

“While consumer IM systems are extremely useful tools, they carry with them the potential for creating havoc in a corporate environment. A file downloaded through IM typically bypasses all of the anti-virus and other defenses set up to protect against threats that might enter the corporate network. Users can send confidential or other sensitive information out through consumer IM systems, bypassing policy enforcement systems that might be in place. In short, consumer IM bypasses corporate defenses.”

**Osterman Research, 2005**



The simplest action you can take to limit IM traffic is to block the associated ports at the firewall. Unfortunately, that's not sufficient to completely block these applications. Developers realized many organizations are blocking IM and have created workarounds that allow [IM] to bypass filters by tunneling traffic through commonly used ports

TechTarget, May 2005

#### The Four Stages of Business IM Usage:

- 1) **Awareness** – "IM is not an issue, we don't use it"
- 2) **IM Blocking** – "Actually employees are using it, we can't control it, so lets block it completely"
- 3) **Corporate IM** – "Employees are finding ways to bypass IM blocks because it's so convenient, so let's install an internal corporate IM system instead"
- 4) **Secure** – "Employees are still using public IM, but incoming IM worms risk cross-infecting the corporate IM system, so lets finally secure the public IM systems that employees need to use anyway"

Did you know? – More than 200 million employees worldwide are using IM, and it's growing fast with projected growth to nearly 600 million by 2008 (Radacati Group)

Did you know? – 90% of organizations surveyed have IM in their corporate networks and 25% of all email users also use IM (Osterman Research)



By storing emails and IMs in the same archive system, businesses can “gain the benefits of a consistently applied policy: a single place in which to perform supervision activities; a reduced number of locations in which to undertake discovery; and reduced training requirements.”

Erica Rugullies, Forrester Research, Information Age 2005

### Governance & Compliance environment:

As the scale and scope of email and IM usage has grown they have become a de facto “record repository”. Often, business transactions are conducted entirely through email or IM. Companies are recognizing the need to enforce corporate policies around messaging in order to protect the organization from human resources issues, litigation, insurance claims, contractual disputes and loss of intellectual property.

Failure to stop inappropriate messages, or to save and then later produce relevant messages, can also lead to prosecution and huge monetary fines.

**Regulations:** The US Sarbanes-Oxley Act requires public companies to archive every record that informs its audit process – email and instant messages included.

The Health Insurance Portability and Accountability Act (HIPAA) and SEC Rule 17a-4 require specific industries and healthcare organizations to save email and IM transactions. Not only must email and IM be saved, they must be readily accessible for investigative or legal discovery purposes.

In the UK the Combined Code of Corporate Governance, the Basel Committee on Banking and the Data Protection Act all have similar implications. The Freedom of Information Act requires public bodies to supply requested information within 20 working days.



\$1.4 billion in collective fines were issued to large Wall Street brokerages in 2003 through non-compliance with regulations

Washington Post

### Governance & Compliance confusion:

Given the large numbers of email and instant messages (one expert estimated a large New York bank would have to retain over 300 million instant messages every year), it's not surprising that many companies are confused and uncertain about how to:

- Establish archiving policy & procedures to minimize costs while covering liabilities
- Implement and manage an archiving policy
- Plan storage and infrastructure
- Provide the right level of skilled staffing

Did you know? – A recent study of small securities firms showed that:

- 36% were not yet archiving email
- 20% were not even aware of regulatory archiving requirements

## What are the key Requirements?



"The trend to integrate messaging security solutions will continue, driven by an increasing number of organizational requirements for messaging security focused on stopping malware, spam and phishing attacks; plus adding secure messaging, archiving, content filtering for compliance and other services."

Osterman Research, 2005

### Key Requirements – Security

There is a clear requirement and duty to provide and maintain security for the organization against the various threats presented by email and IM.

The traditional approaches of separate firewalls, anti-virus, anti-spam, and denial of service solutions can be very resource-hungry to manage. This approach also requires an educated and cooperative workforce, and is hard to keep up-to-date across the organization.

**An integrated, multi layered approach to security is required, including:**

- Virus/Worm detection and deletion
- Spam elimination
- Instant Messaging authentication against corporate identities
- Directory harvest blocking
- Anti-Phishing
- Connection and content threat management



Growing concerns associated with employees' written actions are forcing companies to monitor e-mail more closely than ever

CIO Today

### Key Requirements – Compliance

The ability to quickly and accurately recover all relevant communications on a particular issue is key to compliance and legal discovery. Also important are the abilities to block offensive or inappropriate communications, both into and out of the organization, and to be able to authenticate all relevant communications (prove they had not been altered since sending/receipt, prove the identities of the senders/recipients, and the dates involved).

The organization needs to enforce email and IM usage policies, including archiving of messages, to assure legal and regulatory compliance across the enterprise for both inbound and outbound message content and attachments.

### To facilitate compliance in messaging, organizations need to have:

- Policy based email and IM management strategies – with a granular framework that automatically enforces policy
- Content analysis and management
- Techniques for dealing with encrypted communications
- Archiving of email and IM messages based on global, group or user requirements
- Discovery and rapid retrieval strategies



Email and IM communications are vital to the organization and their availability 24/7 is demanded

### Key Requirements – Availability

Email and IM communications are vital to the organization and their availability 24/7 is demanded, as is the ongoing integrity and security of that communication.

Load balancing, redirection, failover and spooling should be in place to ensure the uptime, responsiveness and message integrity regardless of traffic volume or complexity of your environment. Message archiving provides message redundancy in the event that a mail server crash causes messages to be lost.

#### Ongoing availability requires:

- Message Routing Logic
- Disaster Recovery
- Email Continuity



Centralized visibility and real-time command and control of the entire enterprise messaging flow and management is essential

### Key Requirements – Visibility

Centralized visibility and real-time command and control of the entire enterprise messaging flow and management is essential. This is particularly important bearing in mind the increasing propagation speed of attacks.

Real-time message monitoring, alerting, and comprehensive reporting are required to enable administrators to maintain an overview at the top level and dig into server, location or user specific details.

To minimize administrative effort, users need the flexibility and convenience of examining quarantined messages and self-managing acceptable communications within policy limits. Overall access should be governed to prevent malicious activity within the organization, while enforcing policy for outgoing communications.

### Good visibility and administration requires:

- Centralized management for the whole messaging platform
- Real-time dashboard and alerts
- Reporting & Supervision mechanisms
- Granular Access Controls



When managing your own software based solution, speed of response has to be questioned. With the proliferation and blending of threats at ever increasing rates, can you really stay on top of the latest developments?

### What are my Options? Software based solutions

These are the traditional, software based solutions available from a variety of vendors. In order to provide effective anti-virus, anti-spam, anti-malware and firewall protection, a whole variety of products need to be deployed and built into a 'solution stack'.

These solutions are often tiered across multiple servers, using content filtering software, and anti-virus products from several vendors, together with custom code.

**It's obviously possible to build an enterprise solution this way, however:**

- Selecting, integrating, maintaining, and updating this type of solution across email and IM is time consuming, expensive, and can be very IT resource hungry
- The effectiveness of each solution varies according to the talent of the team that built it – and the resources available to maintain it
- Compliance and archiving are still outstanding issues
- Speed of response has to be questioned – with the proliferation and blending of threats at ever increasing rates, can you really stay on top of the latest developments?



Appliances need to be kept continuously up-to-date and managed – the IT department may feel 'more in control' but is this the best use of their time and skills?

### What are my Options? Appliance based solutions

Appliance based message cleaning solutions combine anti-virus and content filters with network based controls. Generally built on hardened versions Unix or Linux systems they serve as the mail transport agents (MTAs) in organizations' demilitarized zones (DMZs).

Appliances deal proactively with spam using network based sender reputation and outbreak services. Remaining threats are subjected to a variety of filters: Bayesian, heuristic, cluster and rule based. You can build black-lists / white-lists and control your own security.

#### Appliance based solutions can work well, however:

- Appliances are required at each and every entry point – and to provide redundancy and load balancing, back-up appliances are also required
- Appliances need to be kept continuously up-to-date and managed – the IT department may feel 'more in control' but is this the best use of their time and skills?
- Updating and maintaining appliance based solutions across both email and IM can be time-consuming and error-prone
- Compliance and archiving are still outstanding issues



“Why should I filter out this garbage at my end? Outsource as much of the day-to-day busywork as you can, as soon as you can”

Gartner, Network World June 2005

### What are my Options? Integrated Managed Services

Managed Service providers intercept inbound messages and filter out spam and malware before sending sanitized messages on to clients. Quarantined messages are held by the service provider, providing access if necessary, but not requiring the organization to accept, store and manage large volumes of unwanted messages.

Similarly, outgoing messages may be subject to policy enforcement, including facilities such as:

- Virus scanning – no-one wants to pass a virus to their customer
- Content and attachment management – avoiding loss of intellectual property
- Compliance footer insertion

By outsourcing message management, the cleaning and filtering occurs ‘in the cloud’ rather than in the organization’s own DMZ. With an integrated message management solution, administrators benefit from greatly enhanced and streamlined control through a single management console across messaging types. This delivers granular controls and unified visibility across even the most complex messaging environments.



“Managed services’ economies of scale, agility and internet-wide vista confer an advantage that appliances cannot match. The best managed services offer tiered high-availability features and/or uptime guarantees.”

Yankee Group, 2005

### Advantages of using an outsourced service for message management

- **Latest Technology** – You gain the benefit of the most up-to-date and advanced blocking and filtering technologies, which are beyond the budget of many organizations
- **No Hardware / Software** – There’s no need to plan for or purchase additional hardware or software to implement your email & IM security solution
- **Backup and Redundancy** – Any problems are taken care of by the service, and a good service will have redundant hardware and software with failover to eliminate the impact on your incoming and outgoing mail
- **First Line of Defense** – The service is your initial defense in a multi-layered messaging security plan; you can still implement internal security controls to work in conjunction with it
- **Archiving and Compliance** – some services are now offering this feature – your email and IM records are held securely off-site, available whenever you need them. Discovery systems enable rapid identification and recovery of archived messages when necessary
- **Speed of Response** – Because managed services handle large amounts of traffic from multiple clients, they can analyze and identify new security threats and trends before they are published and before your internal security mechanisms would be able to protect against them



Enterprises should evaluate their service provider on its experience, breadth and depth of offerings, reputation, network reach, global footprint and ability to provide an end-to-end solution that secures the entire infrastructure

Bob Blakley of MCI, Computerworld

### Choosing an Integrated Message Management service

Choosing a message management service should involve the following criteria

- **Integration:** Are all of the service provider's pieces of functionality well integrated, delivering a coherent, complete service
- **Scale:** Though smaller service providers may be keen to offer great deals, there are significant benefits to choosing a large scale service provider. The higher the volume of messages processed, together with the diversity of client messaging environments handled, drives increasing experience within the service technical team. This in turn delivers better protection and more rapid reaction to new threats
- **Stability:** A stable, financially sound organization has the resources to develop and fulfill a comprehensive service roadmap that will cater for your evolving messaging needs
- **Functionality:** The service should provide the flexibility to provide the level of service you need – no matter how complex your requirements are
- **Capacity:** Your messages should never be delayed by malicious Internet activities such as spam, virus and worm storms
- **Satisfaction:** Are customers of the service provider happy with the service and technical support. Do they renew with the service provider
- **References:** Can you speak to existing clients of the service provider



The time has come for Integrated Message Management from Postini.  
Security, Compliance, Availability, Visibility.

### Conclusion

For most organizations, email and IM security and management is a perfect candidate for outsourcing.

- Software-only solutions soak up internal resources, are too slow to react and no longer make good business sense
- Appliance based solutions still need maintenance and ongoing upgrades; they require businesses to plan and manage failover, capacity and redundancy; and do not offer the essential archiving options of a managed service
- An integrated message management service provides cutting edge technology, a multi-layered approach, with 24/7 protection, and the archiving facilities to ensure compliance
- The returns on investment of a managed service over in-house point solutions are compelling

"Postini's customers rate them as excellent for almost all metrics gathered in the study, positioning Postini as the lead vendor of Network Application Security products when it comes to customer satisfaction. [...Their] customers are not considering alternatives. In fact we found the opposite to be true, as enterprises using other solutions are considering switching to Postini."

**Henry D. Nisenbaum, TheInfoPro**

## GLOSSARY OF TERMS

### **BOTNET:**

A number of computers that have been set up to forward transmissions (including spam or viruses) to other computers on the Internet, without their owners' knowledge. Such computers are referred to as zombies.

### **DIRECTORY HARVEST ATTACK:**

Designed to probe email directories and harvest legitimate email addresses that then receive even more spam. Directory harvest attacks cause email servers to use valuable resources responding to thousands of bogus address requests, slowing the delivery of legitimate, business critical messages.

### **FALSE POSITIVE:**

Occurs when an anti-spam filter confuses a legitimate message with spam and mistakenly blocks the message from reaching its intended recipient.

### **IP BEHAVIOR ANALYSIS:**

A technique which detects that certain IP connection patterns are indicative of malicious behavior, enabling connection blocking without needing to see the actual message.

### **REAL-TIME BLACK LIST (RBL):**

A list of IP addresses whose owners refuse to stop the proliferation of spam. Many anti-spam products and services use RBLs. However, spam attacks now use zombie networks to evade RBLs, meaning that IP behavior analysis is far superior.

### **SENDER ID:**

A proposed method of eliminating spam, backed by Microsoft and other industry players, rests on the assumption that legitimate email senders will register their IP addresses, and that an email source that does not match a registered IP address should be rejected. However, email authentication proposals to date have proven to be both impractical and inherently flawed.

### **SPAM:**

Unsolicited electronic mail messages, regardless of content, are considered spam. The term can also be used for "junk" postings left on message boards and newsgroups. Spam usually takes the form of bulk advertising.

### **SPIM:**

Spam over Instant Messaging.

### **MALWARE:**

(for "malicious software") is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, trojan horses, and any programming that gathers information about a computer user without permission.

### **PHARMING:**

Similar in nature to phishing, pharming attempts to obtain personal or private information through domain spoofing. Rather than using messages that deliver URLs to fake websites, pharming 'poisons' a DNS server, resulting in a browser request being redirected to the fake website.

### **PHISHING:**

Refers to a false web page or other trojan horse intended to trick users into giving up their credit card, account password or other valuable information. These attacks are frequently propagated by email and increasingly by instant messages.

### **TROJAN:**

A destructive program that masquerades as a benign application. Unlike viruses, trojans do not replicate themselves but they can be just as destructive. Often used to turn a PC into a zombie.

### **VIRUS:**

A program or piece of code that is loaded onto a computer without its user's knowledge and runs against their wishes. Viruses can also replicate themselves.

### **WORM:**

A program or algorithm that replicates itself over a computer network and usually performs malicious activities, such as using up the computer's resources and possibly shutting the system down. Often propagated via instant messages.

### **ZOMBIE:**

A computer which has been hacked into – usually by instant message or email-delivered malware – and is being used by the hacker to launch an attack or spam at other computers – usually without the knowledge of the computer's owner. Networks of zombies are sold to spammers so that Real-Time Black List blocks are evaded.

## Postini – Integrated Message Management

30,000 Businesses Served, 8.3 Million End Users, 3 Billion Messages every Week.

### About Postini

Postini is the global leader in Integrated Message Management, providing security, compliance, availability, and visibility solutions for corporate email and instant messaging systems. Postini's messaging services are designed to protect businesses from a wide range of IM and email threats, address regulatory compliance requirements, and enable the management and enforcement of enterprise policies. Protecting electronic communications for more than 30,000 businesses worldwide, Postini provides comprehensive, flexible, and trusted managed services for message security and management.



### Corporate Headquarters

Postini, Inc.  
959 Skyway Road, Suite 200  
San Carlos, CA 94070, USA  
Toll-free: 866.767.8461  
Phone: 650.486.8100  
Email: [info@postini.com](mailto:info@postini.com)

### EMEA Headquarters

Postini UK Ltd.  
New Loom House, 101 Back Church Lane  
London, E1 1LU, UK.  
Tel: +44 (0)207 082 2000  
Email: [info\\_emea@postini.com](mailto:info_emea@postini.com)

[www.postini.com](http://www.postini.com)

Copyright 2005 Postini, Inc. All rights reserved. Postini, the Postini logo and Postini Perimeter Manager are trademarks registered trademarks or service marks of Postini, Inc. preEMPT is a trademark of Postini, Inc. All other trademarks listed in this document are the property of their respective owners.