White Paper

metagroup.com • 800-945-META [6382]

April 2004

Comprehensive Messaging Management:

A 2004 Imperative

A META Group White Paper
Sponsored by BT

"Given the criticality of e-mail to the success of an organization, enterprises must use appropriate management strategies to ensure the stability and security of the platform. Therefore, enterprises must evaluate their overall e-mail management needs and pursue strategies that maximize protection and control, yet minimize operational overhead."

Contents

Executive Summary

E-mail has emerged as the premier business communications tool of the 21st century. Users routinely cite multiple reasons why e-mail is preferred over the telephone, such as the ability to communicate with multiple parties at one time, the ability to interact at any time, and the generation of a written record. In fact, a 2003 META Group survey found that 80% of business people preferred e-mail over the telephone on a daily basis.

The value of e-mail is intuitively obvious to those who regularly manage mail systems: even brief system outages are met with howls of protest from users, who feel incapacitated without access to colleagues and the resources inside and outside the enterprise. For organizations of all size, e-mail has become an invaluable tool for internal communications, for partner and supplier relationships and for customer interaction. Most of this communication is person-to-person, but there is also a broad spectrum of computer-generated business-critical e-mail that companies rely on.

But the broad reliance on e-mail by the business community has a dark side. Threats to the messaging system are varied and widespread. Viruses and worms continue to wreak havoc on e-mail systems far and wide: we estimate that up to 45% of businesses in 2003 were financially impacted by mail-bourn viruses. Spam, which was nothing more than a nuisance two years ago, has now reached epic proportions, with more than 70% of Internet e-mail traffic thought to be unsolicited commercial e-mail. On a daily basis, spam threatens the usability of e-mail systems by clogging inboxes, consuming storage and transport resources, and exposing users to fraud and security threats.

Viruses and spam, however, are only the most obvious examples of the threats to the health of a messaging system. Hackers now use denial-of-service attacks on the SMTP gateway to bring down mail systems, and spammers launch massive attacks against these same gateways to harvest names for spam mailings. Furthermore, concern about sensitive corporate information traveling over the Internet has led companies to consider options for securing e-mail traffic.

Corporate concerns over e-mail, however, are not limited to threats. An aggressive new regulatory climate means that companies are required to archive and/or supervise e-mail communications. Industries such as financial services and healthcare, as well as the government sector, now have to pay strict attention to ensure compliance with regulations, and broad-based laws such as Sarbanes-Oxley apply to all public companies.

Furthermore, human resources department concerns about circulation of material such as pornography or offensive humor through the mail system has led many companies to investigate tools for monitoring content. The legal department is wary of hostile lawsuits generated by people offended by this material. But legal concerns are not limited to offensive material: corporate counsel may also want to append message disclaimers to outbound mail for added legal protection, and legal counsel must oversee regulatory compliance issues.

Consequently, the management systems required to create a stable and secure messaging system are numerous and complex. The complexity of managing the mail system is exacerbated by the fragmented nature of the vendor community. Most e-mail protection and control suppliers are small and focus only on a few areas of mail management. Therefore, enterprises that take a comprehensive approach to securing and stabilizing the e-mail platform typically use multiple products, which creates operational inefficiencies, thereby raising overall e-mail ownership costs. A fragmented e-mail tool portfolio also makes it impossible to easily establish and enforce corporatewide policy for message management.

Yet we believe the vendor community for mail management is changing rapidly. We foresee the emergence of much broader suites of management tools with a common management and policy engine creating operational efficiencies for mail managers and enabling fine-grained e-mail policy control. In addition to vendors themselves offering more comprehensive product portfolios, we also expect vendors to introduce management platforms to which other third parties can write, creating a flexible heterogeneous vendor environment coupled with a common management and policy engine.

Given the criticality of e-mail to the success of an organization, enterprises must use appropriate management strategies to ensure the stability and security of the platform. Therefore, enterprises must evaluate their overall e-mail management needs and pursue strategies that maximize protection and control, yet minimize operational overhead.

Section 1: Immediate E-Mail Threats

We divide mail management services into two categories — those that immediately threaten the stability of the messaging system and those that are critical, such as secure messaging or complying with regulations, yet do not actively threaten system stability.

Immediate threats to the messaging system include the following.

Viruses

Despite broad efforts to protect against mail-borne viruses and worms, enterprises are still struggling to stop outbreaks effectively. We estimate that up to 45% of large organizations have been economically impacted by a virus attack in the past 12 months. E-mail remains the primary channel of attack. Viruses are starting to appear faster than organizational ability to patch vulnerabilities or disseminate signature files for thousand of PCs. The notorious winter 2003/04 Bagle virus, for example, released nine variants in less than a week. Like many other current viruses, Bagle self-propagates by exploiting e-mail addresses mined from desktop files and by using its own SMTP mailing engine.

Antivirus vendors have noted that the level of virus activity in early 2004 indicates that the year will prove to be the most prolific ever for virus writers. During recent outbreaks, as many as one in five messages was possibly a virus. Viruses also have increasingly disruptive payloads: Mydoom not only launched denial-of-service attacks on commercial Web sites, but also actively deleted files from user desktops. In addition, Mydoom created a remote-access backdoor, allowing hackers to steal personal information (e.g., credit card numbers, passwords), remotely control the PC, or upload malicious code. Therefore, organizations must maintain extreme vigilance against viruses to ensure stability of the messaging infrastructure.

Spam

The rapid proliferation of spam has been without precedent in the history of computing. What was merely a nuisance to most organizations two years ago, has now become an insufferable burden, flooding in-boxes, clogging routers, and consuming vast amounts of storage and bandwidth. For some users, spam has cut productivity as they struggle to separate legitimate mail from commercial e-mail. Furthermore, the salacious nature of some spam messages creates a human relations problem, as users complain about continual exposure to offensive material. We estimate that about 70% of inbound Internet traffic is spam, and that percentage is expected to rise. Therefore, for most organizations, combating spam is the number-one mail hygiene priority.

Along with the basic problems associated with spam, other related threats must be addressed:

- ***Dictionary attacks:*** Also known as harvest attacks, these are a scripted series of delivery attempts whereby spammers send large volumes of mail with likely names to a specific domain to see if messages are bounced or not. In this way, hackers harvest real user names for spamming purposes. Typically, a spam flood occurs directly after a dictionary attack.

- ***Phishing:*** This is a nasty form of spam through which a message appears to be from someone in a position of authority (e.g., bank, retailer) asking for sensitive data such as passwords, credit card numbers, social security numbers, or other personal information, which is then used for various criminal purposes. Phishing activity is growing rapidly and will require different strategies to protect users.

Denial-of-Service Attacks

These attacks refer to basically any hacker action that prevents use of any part of the e-mail infrastructure. Following are details on the most common types of denial-of-service attacks:

- Buffer overload attacks happen when hackers stuff thousands of characters into server memory, along with an executable program with a destructive payload. Hygiene servers need to block buffer overload attacks by locking down open fields.

- Mail floods incapacitate message transfer agents by sending more mail than the server can handle. Companies need to have multiple queues to handle the flood as well as alerting tools to help the mail manager identify the attack and block the domain. Flow control, or tarpitting, can also block mail floods.

- Mail loops (not malicious in intent) can occur when users set up a rule to forward messages to another mail account, which may also have a rule to forward mail back to that account, so the forwarded message is continually bounced. Like mail floods, mail loops can shut servers down when transaction logs run out of disk space. Hygiene servers should contain services that prevent mail floods (e.g., prohibit auto-reply, set maximum hop counts).

Section 2: Proactive Mail Management

After dealing with immediate threats to the stability of the messaging infrastructure, organizations need to look at the broad range of message management tools that will offer added security and stability to the e-mail system. These options range from encrypting messages for more secure travel over the Internet, to archiving e-mail to meet internal and external requirements.

Securing E-Mail

E-mail's vast popularity has created a burgeoning requirement to send mail securely over the Internet. Sent unencrypted, Internet e-mail is susceptible to interception by casual or targeted efforts. Therefore, most organizations have a prohibition against sending sensitive information over the Internet, which has had two results: 1) users ignore the policy, thereby creating a security risk; and 2) users find more costly (e.g., overnight package delivery services) or less-efficient/convenient communication mechanisms (e.g., phone or face-to-face meetings). Heightened commitments to business-to-business and business-to-consumer interaction are creating even more demand for secure message delivery.

Furthermore, grudging governmental and non-governmental regulatory approval of e-mail communication (e.g., in the financial, law, and healthcare industries) often comes with the requirement to encrypt mail. We recommend organizations have a comprehensive plan for e-mail security, encompassing encryption, authentication, and non-repudiation. Organizations must first establish a security policy for what is appropriate to send over the Internet via e-mail. The next step is to determine the constituency being served, because the solution for each combination can be vastly different. For example, enabling board members to swap e-mail securely with internal officers is a different problem from enabling internal users to send secure mail to an ad hoc group of external recipients.

Message Signing

One of the ways spammers create user interest in messages and thwart filter defenses is through use of false information, such as return addresses — a process known as spoofing. Therefore, organizations are rightfully concerned that their legitimate domain name may be misused by spammers. One of the vehicles for combating spoofing is to sign messages digitally, so the signature can be compared against a table that tracks the domain with the appropriate signature. In this way, recipients can be sure that the message sender is legitimate and is not a spoofed domain. We expect digitally signing of messages to become commonplace as organizations seek to more aggressively protect domain identities and combat spam.

Content Filtering

The exponential rise in e-mail volume has led to increasing corporate exposure to the ill effects that an unregulated content transmission engine can bring, including unauthorized disclosure of trade secrets and circulation of offensive material (e.g., sexist, racist) that can expose a company to user-initiated hostile workplace lawsuits. Therefore, companies should install e-mail monitoring and filtering engines to alleviate many of the potential problems brought on by unfettered mail communication.

Archiving E-Mail

Most IT groups are engaged in a battle with end users, whereby the users demand increased e-mail storage allotments to store valuable e-mail, and IT groups argue for minimal storage allocations to reduce cost, decrease e-mail server recovery time, and shorten backup windows. Archival systems offer a compromise, with messages being offloaded from production e-mail servers to alternative stores, while the messages remain readily accessible to users. It is a given that regulated industries must adopt sophisticated archival systems (as well as auditing or surveillance systems — see below) to comply with regulations. The real question is whether non-regulated industries should use e-mail archival services.

Companies in favor of archival systems should consider using them for only a certain category of users (e.g., management, research) or processes (e.g., product development) to lower expenses and limit legal exposure. Regardless of whether an archival system is being used or not, IT groups, along with HR, legal, and management groups, must be able to articulate and defend the corporate policy on e-mail retention (including local and centralized e-mail archiving). Companies must examine the repercussions of not offering archival services — for example, will users find workarounds (local archives, detaching to a file system, printing out documents), and if so, what corporate policies will address these actions?

Organizations using archival systems also need to set policies on handling confidential e-mail (e.g., salary, health issues) as well as ensure that organized-labor rules for privacy/monitoring are followed. We believe this issue will be resolved during the next several years in the following ways:

- Forced by rigid policy enforcement, Global 2000 companies will adopt sophisticated archival solutions to meet regulatory requirements.
- In non-regulated industries, the pro-purging force — citing legal concerns — generally will triumph, meaning purge cycles will be short (e.g., 60 days for the

inbox) and mailbox sizes will be kept under 100MB. By 2006, about 15% of non-regulated Global 2000 companies will use archival systems to enable users to retain large amounts of e-mail — particularly attachments — without stressing the production e-mail system.

- New compression technologies and attachment-handling services (e.g., offloading attachments to a separate store) will emerge, which will enable users to store more e-mail while staying within mandated storage allotments.
- E-mail metadata (e.g., tracking e-mail subjects) will be captured for knowledge management purposes, rather than the e-mail itself, thereby avoiding long-term retention of actual messages.
- We expect e-mail regulatory requirements to be extended to instant messaging, leading vendors to broaden the scope of electronic communication coverage.

Therefore, enterprises need to balance the needs of various constituencies and determine an appropriate message archival strategy, along with purging and mailbox storage guidelines. These actions should be coordinated with a broad e-mail management strategy.

E-Mail Regulatory Compliance

Financial institutions have long been subject to e-mail archival and surveillance guidelines from various bodies such as the US Securities and Exchange Commission (SEC), the New York Stock Exchange (NYSE), and the National Association of Securities Dealers (NASD). Yet our research indicates that many firms ignore the regulations, and other companies have a wide range of interpretations of how compliance should be carried out.

Many organizations are re-examining e-mail regulations and compliance efforts after seeing several high-profile cases where companies were subject to multimillion-dollar fines for non-compliance. Financial institutions are not alone: US state, local, and federal government bodies may be subject to retention requirements under the Freedom of Information Act. Insurance companies, often at the state level, have e-mail regulatory requirements, and parts of the process manufacturing ecosystem (particularly for environmental adherence) are subject to e-mail regulations.

Furthermore, newer, broad-based acts such as the USA PATRIOT Act, the Sarbanes-Oxley Act (for corporate governance), the Health Insurance Portability and Accountability Act (HIPAA), E-SIGN, the Uniform Electronic Transactions Act

(UETA), and the US Food and Drug Administration Title 21 of the Code of Federal Regulations Part 11 have rules that govern e-mail disposal and interaction.

It is under this climate that we believe the market for e-mail regulatory compliance will flourish during the next five years. Generally, regulations address three areas:

1. Archiving older messages for a specific period of time, to create a paper trail
2. Supervision of messaging, to prevent abuse
3. Auditing, to ensure that messages are not tampered with and that review efforts are carried out

Enterprises must ascertain what e-mail regulations they are subject to and deploy appropriate technology for meeting those requirements, optimally as part of an overall e-mail management strategy.

Section 3: The Importance of the Mail Transfer Agent

At the heart of any mail system is the message transfer agent (MTA), which routes messages to and from the Internet. This is typically a dedicated server which works with internal routing servers such as Domino or Exchange. However, only recently have most organizations given thought to their MTA strategies due to numerous events, including the following:

- Legitimate message volume has risen on average 15%-25% annually during the past few years, driven by greater volume of messages, the increasing size of messages, and more messages with ever-larger attachments, forcing capacity upgrades.

- The increased criticality of e-mail to an organization has risen rapidly, forcing organizations to add MTA redundancy.

- Spam and malicious attacks (e.g., denial of service, name-harvesting schemes) have forced organizations to consider MTA-based services for added protection.

- E-mail marketing campaigns have resulted in demands for extremely large capacity requirements and marketing-specific features (e.g., improved bounce-back handling).

Consequently, most organizations should re-evaluate MTA needs and suppliers as part of an overall reassessment of mail management concerns. At the very least, organizations must be proactive in staying current with relay versions and patches, which are being presented with increasing frequency as new

vulnerabilities are identified (e.g., remote root exploit), and hardening operating systems to protect against system software vulnerabilities, which can be used to bring down mail systems.

The future of mail relay services will tend toward commercial products with easier-to-manage feature sets and a broad spectrum of other capabilities (e.g., virus, spam blocking), as organizations focus more on end-to-end messaging performance and hygiene. Increasingly, there will be a distinction between pure relay duties (e.g., routing-table management, mail-list expansion, address rewrite) and a policy relay layer, which provides services such as quarantine, filtering, reporting, flow control, and MTA acceptance rule enforcement. Therefore, we recommend that organizations re-evaluate MTA services to ensure that feature sets keep up with rapidly evolving requirements and that MTA strategies are synchronized with overall e-mail management programs.

Section 4: Message Service Delivery Models

When contemplating e-mail management services, organizations must determine the appropriate deployment model — either a hosted model where services are performed external to the organization, or an on-premises traditional software/hardware gateway approach. With the hosted model, organizations redirect their e-mail to the hosted vendor, which processes the e-mail and then relays it to the subscribing company. Typically, organizations choose a hosted model for the following three reasons:

- ***Time to value:*** Hosting services can be up and running in as little as a week, compared with on-premise tools, which may take months for IT staff to load, tune, and test the software.
- ***IT resources:*** Organizations with scarce IT resources may be loath to add yet another duty to an overburdened IT staff. Hosted services require only light IT group oversight.
- ***Payment options:*** Organizations eager to avoid capital expenses favor the predictable monthly fee charged by hosted suppliers, which also makes internal chargeback easier.

To these traditional reasons, we add one more due to market immaturity: companies may choose a hosted service to avoid investing in a tactical on-premises tool. By using a hosted service for two or three years, the company can then move directly to a strategic on-premises supplier.

The reasons most organizations choose an on-premises model are tradition, security concerns (e.g., some hosted vendors handle e-mail only in memory, while others write it to disk), control, customization, and cost. Overtime, we believe companies may use a combination of on-premises and hosted services, with the hosted vendor providing message caching (when the downstream MTA is offline) and/or disaster recovery services, while the on-premises tool may be doing local compliance and archival functions. We also anticipate that organizations may switch from hosted to on-premises suppliers, depending on the prevailing attitude toward outsourcing or availability of resources. These two dynamics suggest that the optimal approach is to use a vendor that can supply both hosted and on-premises services.

Section 5: Creating E-mail Management Efficiencies

Given the vast scope of e-mail disciplines required to ensure a secure and stable messaging system, enterprises must take steps to ensure low operational costs, efficiency, effectiveness, and reliability. We believe there are several factors that will drive down long-term e-mail management costs.

Physical and Logical Centralization

Since many e-mail architectures are based on the limited scalability of earlier client/server mail systems or even shared-file mail systems, many topologies are characterized by low server-to-user ratios (e.g., <500 users/server). With the advent of much more scalable mailbox servers, bandwidth-sensitive clients, advanced compression services, and dropping bandwidth prices, companies should consider physically centralizing e-mail servers where it makes economic sense (basically trading the cost of a local server versus bandwidth).

In addition, when physical centralization is not desirable, enterprises should consider logical centralization of mail management activities, where a core team of e-mail specialists manages all central and remote servers from one to three data centers. We believe this centralization creates operational economies of scale by enabling consistent management practices across a large number of users. This allows, for example, common upgrade testing, troubleshooting, and spam filter configuration across the enterprise.

Policy-Based Management

Because the requirements for managing and controlling end-user and group message traffic are so varied, it becomes an exercise in complexity to control diverse user accounts granularly. We believe policy-based management of users and groups will be the approach companies ultimately use to cope with the chaotic situation of applying diverse controls. Using a flexible directory (preferably the

native mailbox store or a synchronized LDAP directory), managers can, for example, apply different archival policies for regulated and unregulated parts of the business, assign different spam control features based on user tolerance or job function, or delineate different requirements for secure messaging. Therefore, the more mail control functions that can be managed and maintained under one common policy engine, the more exact the control and the more efficient the operations. A common policy engine also makes auditing and change management a far simpler process.

A Single Console

Similarly, we believe operational efficiencies are generated with a common management console that enables control over a broad and diverse portfolio of messaging management services. With a common console, managers can control numerous services via one common interface — rather then having to toggle between multiple vendor management interfaces.

We see common management consoles coming from two directions:

- Some vendors are broadening their own e-mail management portfolios themselves through in-house development and acquisition, and applying a common management console across all services.
- Other vendors are writing open management frameworks, allowing third-party vendors to use the common management framework. In this case, enterprises can assemble a diverse suite of messaging management products from diverse vendors and gain the operational efficiencies via the common management interface.

Additional efficiencies can be gained if diverse vendor relationships can be maintained via the supplier of the common management framework.

Common Infrastructure

Underlying messaging infrastructure should be examined for operation cost savings. Most organizations have standardized on one e-mail package and have common directory, management, and security services across the enterprise. Therefore, the challenge is to take full advantage of already established infrastructure for ancillary mail management services such as hygiene, security, and archival services.

Establishing end-user quarantine accounts, for example, should be synchronized with the mail directory to avoid dual user account creation or deletion, and passwords should be common or synchronized for user and help desk

efficiencies. Likewise, attachment management and archival services should exploit existing storage infrastructure, such as hierarchical storage management services and storage-area networks. Therefore, common infrastructure use is desirable when selecting e-mail management services.

Section 6: Market Evolution

The current market for e-mail management services is made up mostly of small suppliers. Yet during the next several years, we expect the mail market to change from a small supplier model (currently forcing organizations to stitch together complete solutions from multiple vendors) to an industry dominated by six to nine large vendors that will offer a quasi-complete range of e-mail management services.

These large suppliers will address a panoply of needs, including spam and virus blocking, protection from denial-of-service and other malicious attacks, secure messaging, message control (e.g., expiration; prohibition of forwarding, printing, and saving to disk), supervision (primarily to meet regulatory requirements), archiving, and content/file blocking, all wrapped inside a comprehensive policy enforcement, administration, and management engine. We also anticipate emergence of a healthy hosted market for e-mail hygiene services. Market consolidation of single suppliers benefits organizations in that enterprises will have a common console for most mail management needs, creating administrative (and hardware) efficiencies and facilitating corporate policy execution.

When product functionality is equivalent, companies should opt for larger, multifunction vendors. However, if a strong differential exists, a best-of-breed choice is still appropriate. To maximize management efficiencies, companies should plan to migrate to suites of services during the next several years.

Bottom Line

Corporate e-mail services constitute a critical communications infrastructure that is more appealing than telephone services to most users. Service interruptions not only create loud protests from frustrated users, but they can also impact the ability to deliver services to customers and business partners. At the same time, threats to e-mail services are rising rapidly. Spam can clog gateways and tax many system components, and the volume and destructiveness of viruses is accelerating. Dictionary attacks and various denial-of-service attacks can bring Internet services to a halt, and spammer spoofing can cause PR, availability, and legal hassles. In addition, hackers can flood gateways with junk e-mail, straining system components.

Most organizations currently approach mail hygiene on a piecemeal basis, mostly in a reactive mode. We believe organizations must develop a comprehensive approach to mail management that covers spam and virus protection, denial-of-service attacks, and inbound/outbound content filtering for offensive material and unauthorized intellectual property disclosure, as well as the tools needed to meet SEC, HIPAA, and other compliance requirements.

In the face of these diverse challenges to the e-mail system, organizations must strive to create operational efficiencies in e-mail management. This will happen organically as vendors offer broader product suites that use common management and infrastructure. Vendors will also begin to offer open frameworks to which third-party vendors will plug-in, enabling common configuration and management services across a diversity of vendors. In both cases, we believe operational efficiencies can be generated by enabling mail managers to manage multiple mail management services from a common console and to set granular user and group policies across the enterprise, while improving system effectiveness and reliability. Therefore, companies must strive to create a stable, secure, and compliant messaging infrastructure, while minimizing the operational burden.

Matt Cain is a senior vice president with Content & Collaboration Strategies, a META Group advisory service. For additional information on this topic or other META Group offerings, contact info@metagroup.com.

About META Group

Return On Intelligence[SM]

META Group is a leading provider of information technology research, advisory services, and strategic consulting. Delivering objective and actionable guidance, META Group's experienced analysts and consultants are trusted advisors to IT and business executives around the world. Our unique collaborative models and dedicated customer service help clients be more efficient, effective, and timely in their use of IT to achieve their business goals. Visit metagroup.com for more details on our high-value approach.