

The inherent risks of email

Why no organization should be without a comprehensive email policy supported by Sophos PureMessage

Sophos Inc, USA

September 2003

SUMMARY

Email is a critical medium for communicating, collaborating, and sharing information within and between organizations today. This paper details several risks to which organizations are exposed by unfiltered email, describes topics a company email policy might include, and explains how a message-filtering solution, such as Sophos PureMessage, can effectively support an organization's email policy.

Introduction

The dramatic growth of desktop computers, email, and the internet over the past decade has created a fundamental shift in the way organizations and individuals communicate and store information. While this shift has created several benefits, such as rapid communication and information sharing, it has also created new threats for organizations.

Email is a critical medium for communicating, collaborating, and sharing information within and between organizations today. A full 100% of the Fortune 1000 use email to conduct business, and much of the communication that occurs between an organization, its employees, its customers, and its business partners occurs via email. The importance to organizations is demonstrated by the time their users now spend using email. The average US worker receives at least 30-60 messages per day (with executives receiving significantly more), and spends up to three hours or more on email each day.

Up to 60% of a company's intellectual capital can reside as documents stored by users on its messaging system.

Email not only facilitates communication, but is also a primary medium for document and information sharing and storage. Users often store documents only as attachments in email, rather than saving them to file folders on their workstations or servers. Not surprisingly, it has been estimated that 60% of a company's intellectual capital can be found in its messaging systems.

However, as organizations have placed increasing reliance on email to conduct everyday business, the risks associated with email have also grown substantially. External threats, such as spam and viruses, jeopardize the security of an organization's infrastructure and the productivity of its users. The risk also exists that users may, with the click of a mouse, cause accidental or deliberate harm, such as sending trade secrets to competitors, circulating sexist or racist jokes or remarks, or accidentally sending out personal customer information.

These risks have created the need for organizations to have an overall policy governing the handling and usage of email, to ensure employees understand the policy, and to support the policy with a message-filtering solution.

Email risks to organizations

The risks associated with email include infrastructure security threats (viruses and other attacks), productivity threats (including spam), corporate liability (offensive content), confidentiality breaches, mistakes, and compliance issues.

Infrastructure security

Because sending and receiving messages outside the company requires a connection to the internet, email creates an easy opportunity for malicious external attacks. Viruses and other malicious code (worms, Trojan horses, spyware, etc) are the most common types of attack, and email is the most prevalent avenue for these attacks. A 2002 survey by ICSA stated that email was the means of infection for 86% of virus attacks reported.

When viruses occur, they can cause email or computer system downtime, destroyed data, and security vulnerabilities, which can result in lost revenue and productivity, loss of confidential information, and costs associated with clean-up. Non-virus Denial of Service (DoS) attacks also exist, such as buffer overflow attacks, where a hacker sends attachments with long file names or other unusual or excessive traffic in an attempt to bring down email systems.

Directory Harvest Attacks (DHAs) also present a security threat to organizations. In DHAs, email is sent to thousands of possible addresses at a domain in an attempt to “harvest”, or collect, valid email addresses from an organization. Variations on email addresses are attempted, such as mjones@company.com, maryj@company.com, maryjones@company.com, mary.jones@company.com, ajones@company.com, or bjones@company.com. Addresses that aren’t rejected by the receiving mail server are considered valid, and can be used or sold for spam or other attacks.

Security risks may be more benign in intent. For example, somebody may send a large attachment to many recipients in an organization, causing overload on the organization’s email infrastructure. Infrastructure security can also be jeopardized by internal mail abuse, such as an employee using an organization’s email system to send spam messages. The messages could potentially overwhelm the system or could cause the company’s domain to be blacklisted for spam, resulting in messages not getting delivered to customers or partners who actively filter for spam.

Employee productivity

Unsolicited commercial email, or spam, has become a top email-related concern for organizations. Several estimates indicate that spam represents over 50% of the messages corporations receive today, and this proportion is expected to continue to grow. While often regarded as just a nuisance, spam can actually represent significant costs for organizations. Ferris Research estimates that the cost of spam to US organizations was \$8.9 billion in 2002, accounting for lost productivity, consumption of IT resources, and helpdesk time. Even using conservative estimates, the annual cost of spam to a 10,000-person organization could approach or exceed \$1 million.

Another possible productivity issue is employees using work email for excessive personal use. For example, audio or visual files, such as MP3 or mpeg files, could be sent and received using the corporate email system, consuming bandwidth and storage resources and representing potential non-work activity during work time. Or a person might be sending or receiving excessive email traffic for a home business or other personal purpose during work time.

Email is the most common route for external attacks on an organization by viruses and other malicious code.

Spam represents over 50% of messages received by organizations today, resulting in significant costs of additional IT resources and reduced productivity.

Corporate liability for offensive content

Offensive content received from external sources or circulated internally presents organizations with a liability risk. If employees complain about offensive content and organizations fail to take steps to address it, employees might initiate legal action based on a hostile work environment.

The Civil Rights Act of 1964 prohibits workplace discrimination based on “race, color, religion, sex, or national origin”. This was later interpreted to include environments “that a reasonable person would find hostile or abusive” (Harris v Forklift Systems). More recently, discrimination/harassment cases have been based on offensive email. In 1995, Chevron settled a sex discrimination lawsuit for \$2.2 million, which was based in part on email, including one that listed 25 reasons that beer is better than women (Nardinelli v Chevron). In Strauss v Microsoft, sexually-related email was admitted as evidence, despite Microsoft’s argument that it shouldn’t be admissible.

Companies’ email is increasingly cited in sexual harassment claims, and more than half of all employees surveyed have received inappropriate email at work.

These cases are not uncommon. The ePolicy Institute estimates that more than a quarter of Fortune 500 companies have defended themselves against sexual harassment claims based on inappropriate email and/or internet use, and surveys of employees show that 50-70% have received inappropriate email at work. Such cases are not only costly to defend against legally; they could result in long-term damage to a company’s reputation.

Confidentiality breaches

With so much of an organization’s intellectual capital residing in its messaging infrastructure, as well as the ease with which information can be sent outside the company with the click of a mouse, email presents a risk of accidental or deliberate breaches of confidentiality. For example, a disgruntled or dishonest employee could send trade secrets or insider information to competitors or others. Internal organizational memos of a confidential nature may be distributed outside the company and later posted on external sites or message boards. While other avenues for breaches of confidential information exist, such as copying files to diskettes, email represents one of the easiest means of transferring information outside an organization.

Deliberate or accidental external circulation of confidential or proprietary information by email can result in substantial costs to businesses.

PriceWaterhouseCoopers, the US Chamber of Commerce, and the American Society for Industrial Security (ASIS) International released results from a survey of 138 CEOs about intellectual property and proprietary information in 2002. More than 40% of the respondents indicated that confidential information within their organizations had been lost, with the cost of this type of loss to US business estimated at \$59 billion.

Mistakes

An organization could face legal risks, as well as risks to its reputation, based on employee mistakes. For example, an employee might accidentally attach confidential customer data or information to an email, or may accidentally put all recipients in the “to” or “cc” line of a notification or newsletter, resulting in the widespread distribution of customer, partner, or supplier email addresses. Or an employee might inadvertently forward offensive or sensitive content to a customer, partner, or other party. Other types of confidential information that could be distributed include credit card numbers and copyrighted information.

A few years ago, a string of incidents in which email addresses were accidentally distributed made headlines for companies including Seagate Software (1,500 customer and reseller email addresses), Nissan (24,000 potential Xterra buyer email addresses), and AT&T (1,800 customer email addresses). Another mistake that attracted media coverage involved an FCC employee accidentally sending an inappropriate joke instead of a news report to 6,000 bureaucrats and journalists. These types of mistake can result in a public relations and legal nightmare.

Non-compliance with regulations and internal legal guidelines

If internal legal guidelines are not implemented, the costs of regulatory non-compliance could be significant.

External regulations will vary depending on the company and industry, but they can include US regulations such as the Healthcare Insurance Portability and Accountability Act (HIPAA), for the healthcare industry, the Graham-Leach-Bliley Act (GLBA) for the financial services industry, and US 21 CFR Part 11 for FDA-related industries. Organizations may want to implement archiving or message filtering to protect against non-compliance with these and other regulatory standards and guidelines.

An organization's legal department may set guidelines around email storage and disclaimers on outbound mail, and non-compliance with these guidelines could represent a liability or cost risk. If an organization has a policy of storing all correspondence with the legal department, but does not, it could run the risk of needing a document that is no longer available. Or an organization might have a policy of deleting correspondence after a certain amount of time to minimize the cost of potential legal discovery requests. If this policy is not complied with, the costs could be significant.

Developing and communicating an organizational email policy

The various risks associated with email highlight the need for organizations to develop, communicate, and support an organizational email policy governing inbound, internal, and outbound email communications.

The process of developing an effective organizational email policy should involve representatives from the human resources, legal (with involvement from employment law experts), and IT departments. An overall email policy should be created covering all risks to the organization (including viruses and spam), and address not only the content of the policy itself, but also how it will be communicated, monitored, and enforced. When developing the policy, it is important to consider privacy laws such as the Electronic Communications Privacy Act (ECPA), as well as the policy's effect on employee morale.

Each organization will vary in the specific policies it will want to consider. Some examples of topics that could be covered include:

Communication of the policy to employees

- How will the organization communicate the policy to existing and new employees?
- Will employees have to sign that they understand the policy or prove understanding by passing a test?
- What other aspects of email communication will be explained to employees (e.g. does deleting a message mean it is removed from the system entirely)?

An email policy should not only cover the risks of viruses and spam, but also how policy will be communicated, monitored, and enforced.

Enforcement of the policy

- Which areas of the policy will the organization monitor or enforce?
- Will enforcement be limited to virus checking, or will the organization implement filtering or monitoring for spam, offensive email, confidential information, mistakes, or other areas?
- If enforcement isn't planned initially, is it a possibility in the future?
- How should the potential for monitoring/enforcement, and the relationship of this monitoring with privacy laws, be communicated to employees?
- How will enforcement or monitoring be accomplished?

Security policy

- How does the organization plan to defend itself from viruses and other external attacks?
- If an email contains a virus, what notification will the user or sender receive?
- What attachment sizes and types will be allowed in the organization?
- Will the organization monitor for signs of email abuse?

Spam policy

- How does the organization define spam, and how does the organization want to address it?
- If a spam-filtering solution is selected, how will spam that is identified be handled (e.g. will users have access to the spam)?

Personal use of email

- What level of personal use will be allowed within the organization?
- Will the organization monitor or spot-check for acceptable levels of personal email?
- If so, what will happen if excessive personal use is found?

Offensive content

- Do employees understand discrimination and harassment issues?
- How is offensive content defined?
- What is the process for responding to a complaint about offensive email?
- Will the corporation monitor for offensive content in inbound, internal, or external email?
- If so, what will happen in each case to mail identified as offensive?

Confidentiality

- Is the definition of "confidential" well understood by employees?
- Will the organization monitor for potential breaches of confidentiality?
- If so, how will the list of keywords, or other attributes considered to define confidentiality, be maintained and monitored over time, and what will happen if confidential information is discovered?

Regulatory compliance

- What, if any, external regulations apply to the organization, and what policies and tools are required to comply with these regulations?

Copyrighted material

- Will the organization educate users about copyrighted materials?
- Will the organization monitor for potential unauthorized distribution of copyrighted material?

Email retention policies

- What is the organization's policy for the retention of email?
- How will the organization enforce it?

Disclaimers or other banners

- What, if any, content does the company want to attach to all outbound email for legal or other reasons?
- How will this be communicated and enforced?

Outbound email guidelines

- What other guidelines should be established, either at an organizational or a group level?
- Would these guidelines include how to send mail to many recipients without revealing their email addresses, processes for reviewing important broadcast messages prior to sending, avoiding offensive words in outbound email, etc?

Use of a filtering solution to support organizational email policy

Once the email policy is established, organizations need an email-filtering solution to support it. Examples of how a filtering solution could support the policy include:

- Scanning of all inbound and outbound mail for viruses and quarantining any message found to contain viruses.
- Evaluating inbound messages for spam, then quarantining or marking messages determined to be spam.
- Checking messages for offensive content, quarantining those identified as offensive, and notifying an administrator accordingly.
- Checking outbound messages for subjects or keywords indicating possible IP (internet protocol) breaches, and redirecting the message to an administrator or supervisor for evaluation.
- Adding a standard legal disclaimer to all outbound messages.
- Archiving a copy of all correspondence to or from the legal department.

When selecting an email-filtering solution to support an organizational email policy, several aspects of the solution should be evaluated, including:

- Is the solution able to support a variety of policy needs for various mail streams (e.g. checking inbound mail for virus, DoS, DHA, spam, and offensive content, and processing outbound mail by checking for confidential information, and appending disclaimers)?

- Is the solution effective at catching spam and viruses?
- Is it easy to create, test, and maintain policies specific to the organization?
- Is it easy to select from a wide range of actions when policy rules are triggered (e.g. blind copying someone, quarantining a message, rejecting a message and notifying the sender, forwarding the message, etc.)?
- Does the solution enable understanding and reporting of what rules are being triggered and why?
- Is the solution able to scale to meet large message volumes?

Sophos PureMessage – enterprise email protection

Established, trusted, and proven, Sophos PureMessage protects organizations against viruses, spam, and other email-borne security threats. Combining industry-leading anti-virus and anti-spam technologies with flexible policy management and world-class support, PureMessage is the most comprehensive, flexible and mature mail filtering solution for businesses.

- PureMessage safely removes up to 98% of spam at the gateway, with daily updates and the latest anti-spam techniques.
- Virus-detection tools scan for known and unknown viruses, protecting the network against malicious code.
- Corporate communications policies are easily managed using PureMessage's flexible policy manager, for complete, precise control over mail filtering.
- Quarantine digests enable end users to access blocked messages easily, eliminating false positives.

PureMessage enables large organizations to implement and manage communications policies at the email gateway.

The PureMessage email management solution enables large organizations to implement and manage communications policies easily at the email gateway. The PureMessage Policy Builder interface makes building and managing simple or complex email policies straightforward. These can range from basic "acceptable use" policies restricting the use of offensive words, to high-level protection of confidential trade secrets or the addition of legal disclaimers. The breadth of PureMessage allows any organization to deploy the policies most appropriate to their business needs.

PureMessage includes more than 30 pre-created tests and actions that can be applied to messages, providing extensive flexibility to support organization-specific email policies. Examples of email policies include:

- Blocking or quarantining messages larger than a certain size or with certain types of attachments.
- Archiving messages based on sender, recipient, or content for regulatory compliance.
- Rerouting or quarantining messages that contain inappropriate content or confidential information (sent deliberately or accidentally).
- Adding a standard disclaimer to outbound messages across the organization or for certain users.

Attacks designed to halt email productivity (DoS), and those that steal email addresses as future spam targets (DHAs), represent a growing security threat. PureMessage provides powerful protection against such threats to an organization's email system. Through PureMessage's anti-DoS and anti-DHA filter, sources of attack are quickly identified and can be immediately thwarted. It can ignore future communication from these sources or notify key email administrators that an attack is in process.

PureMessage protects against viruses and spam threats, and supports policy management, enforcement, and monitoring.

Minimizing an IT administrator's workload, PureMessage provides immediate, out-of-the-box protection against spam and virus threats. The configuration and administration of PureMessage is easily accommodated through its web-based administrative interface, PureMessage Manager. PureMessage Manager enables the easy, flexible creation and management of spam, virus, and other policies, and provides reports necessary to evaluate system productivity. Examples of reports include message traffic, top spam sources, quarantine content summaries, and service status information. Central Server Management enables organizations to share PureMessage configurations across multiple servers, providing synchronized policies and consolidated reporting.

PureMessage is the only filtering product that delivers exactly what enterprises need today – the best in spam and virus protection and a policy-management interface capable of protecting against other internal and external threats to an organization.

This white paper is intended for information purposes only and should not be considered legal advice. Legal advisors should be consulted for the development and implementation of any organizational email policy.

SOPHOS INC
North America
Toll free: 1 866 866 2802
Email: nasales@sophos.com

SOPHOS
WWW.SOPHOS.COM

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France • Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Sophos, Inc. All registered trademarks and copyrights are understood and recognized by Sophos.