SOPHOS

Effective email policies:

Why enforcing proper use is critical to security

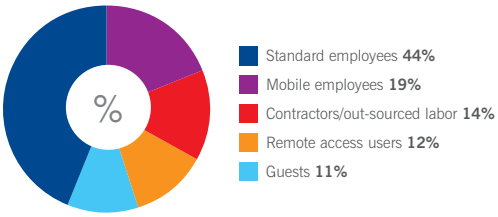
The unmonitored and unguarded use of email by employees poses a multitude of risks to organizations. The distribution of inappropriate or offensive content, malicious emails, and the risks of data leakage all threaten working environments, IT resources and an organization's reputation. A comprehensive, transparent and enforceable email acceptable use policy (AUP), combined with robust email security solutions, dramatically reduces exposure to these risks. This paper investigates why organizations need an email AUP and highlights how they can enforce it. It also provides practical guidance on developing a policy that meets the combined requirements of an organization's IT, HR and legal departments.

A Sophos white paper

April 2008

Effective email policies:
Why enforcing proper use is critical to security

Email is now central to the day-to-day operation of practically all organizations, regardless of size or sector. Yet, while it is far too important to lock down, email poses a large enough risk where it cannot be left unregulated, especially as nearly all employees expect a certain level of personal email use while at work. According to employers, however, it is their own workforces that pose the greatest threat to security (figure 1).



Source: Sophos web poll, Sept 2007

Figure 1: Which user exposes you to the greatest threat?

Acceptable use policy and IT security

While banning staff from sending or receiving personal emails is unrealistic, organizations can set boundaries that define reasonable, excessive or inappropriate use, through a comprehensive, updated and enforced email acceptable use policy (AUP). A well-articulated email AUP addresses four core security and operational areas:

- Compliance
- Safe working environment
- Data leakage
- Asset abuse.

A framework for corporate governance

According to IDC Research 97 billion emails are sent worldwide each day[1], and it is estimated that 80 percent of an organization's operational records are stored within the email infrastructure. Governments around the world have responded to email's growing use as a business-critical tool by introducing increasing levels of legislation governing the security, storage and retrieval of email (see box). Falling foul of such legislation not only damages an organization's reputation, but can lead to fines, market de-listings and, in extreme cases, prosecutions and prison sentences for senior management.

Keeping abreast of such legislation is challenging, and an AUP can help by providing a formal framework that is easily reviewed, audited and enforced to ensure compliance.

Increasing compliance

» Accounting: Sarbanes-Oxley Act (SOX) provides new and enhanced standards for all US public company boards, management and accounting firms.

» Healthcare: HIPAA (Health Insurance Portability and Accountancy Act) established national standards in the US for electronic healthcare transactions.

» Credit cards: PCI DSS (Payment Card Industry Data Security Standard) governs the handling of information relating to credit card transactions.

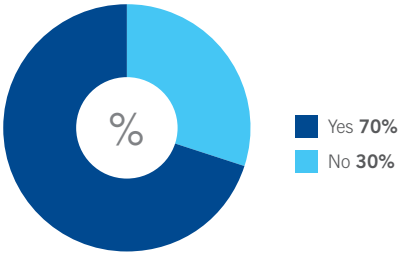
» Data Protection Act: A UK law that regulates the storage and availability of personal details held on computers and other filing systems.

Creating a safe working environment

An email AUP will promote a safe, productive working environment where employees can operate without fear of exposure to illegal, abusive, inappropriate or malicious material, such as pornography, jokes, harassment or threats. By removing ambiguity and ensuring all employees work to the same rules, the policy sets clear expectations on what constitutes acceptable email content.

Preventing leakage of confidential information

According to IDC email is the number one source of leaked business information[2]. Additional research confirms that most organizations are concerned about the loss of sensitive data via email (figure 2).



Source: Sophos web poll, Oct 2007

Figure 2: Are you worried about sensitive data leaking from your email?

Most of the time this can be accidental (thanks to functions like Autofill) with research showing that half of employees have sent a message containing sensitive or potentially embarrassing information by mistake[3]. In addition, analysts The Radicati Group found that 77 percent of users have forwarded business emails to their personal accounts in order to complete work when away from the office[4]. Even this most innocent of practices can leave an organization in breach of compliance regulations and can place commercial information in unauthorized hands.

The perils of "Autofill"

All versions of Microsoft Outlook® since Outlook 2000® allow email users to populate the "to", "cc", and "bcc" message fields automatically. For example, typing a "J" into the "to" field will bring up a listing all of the user's contacts whose first name or surname begins with that letter. While this tool saves time, it also exacerbates the problem of inadvertent data loss as it is relatively easy to send an email to the wrong contact.

Preventing asset abuse

Excessive and/or inappropriate personal use of email wastes bandwidth and places storage archives under strain, impacting on an organization's ability to use its email infrastructure. This is particularly problematic when employees circulate non-critical attachments, such as family photos or videos. Prohibiting or restricting this practice preserves the integrity of the email system and can extend the life of storage solutions. It also ensures that IT staff remain focused on their core responsibilities and do not spend time clearing personal emails from the system.

What an AUP should cover

An AUP should set out exactly how an employee is expected to use an organization's email system, containing prescriptive advice on best practice and clearly defining prohibited behavior.

It is essential that regulations are explicitly stated and easily understood. The content of an AUP will vary between organizations, reflecting their regulatory environment, email quantity, IT resources and culture. Some may choose to incorporate rules governing email use into a wider AUP that covers all technology use, from telephones to web browsing to photocopying.

However, in general, an email AUP covers three main elements:

- Appropriate and inappropriate email use
- Policy enforcement
- Policy sanctions.

A detailed example of a suggested email AUP can be found in the appendix at the end of this white paper*, but areas that should always be covered include:

Inbox management

In response to the continued growth in email use, organizations should attempt to limit the volume of messages stored in employee mailboxes. The number of emails held in archiving systems that capture both internal and external mail should also be limited, ensuring resources are not overloaded and allowing for easy message retrieval.

Circulation of attachments

Users commonly view email as a quick method of sharing content with colleagues. However, this practice needlessly uses up bandwidth and archive space. Instead, all attachments should be removed before an email is stored and saved on an appropriate server. Additionally, employees should be instructed on how to use shared network folders to circulate files internally, rather than attaching them to emails. Consider that one person sending a 5 MB attachment to five other employees results in more than 25 MB of email server storage requirements. Placing this file on a shared server and circulating a link to its location not only greatly reduces the size of the email, it prevents unnecessary duplication of files across multiple locations.

Remote access of email services

Rules should be set governing remote access to the corporate email network, both from employees' own computers and over the internet/public Wi-Fi networks. Some organizations ban this practice altogether, while others permit it only if the computer accessing the network is certified as secure by, for example, a network access control (NAC) solution.

Personal/non-business critical use of email

File types categorized as non-business critical (for example, JPEGs, MP3s, executables and anything considered potentially malicious) should not be received or sent. The dissemination of illegal, offensive or other inappropriate content should also be prohibited. Employees should understand that companies are obliged to report any unlawful behavior to the authorities, and that inappropriate activity can invoke disciplinary proceedings. Some organizations may also choose to block access to web-based email services, such as Hotmail and Gmail.

AUP enforcement

The email AUP must be enforced if employees are to adhere to its rules. If they realize that their messages are reviewed and stored – and then retrieved if needed – employees might think twice before misusing the email system. An AUP should provide total transparency about how an organization intends to police its email system, ensuring that there are no surprises in the event of disciplinary action being invoked.

Enforcement through technology

The key to enforcement is the deployment of IT security solutions capable of auditing everyday email use, spotting and tracking potential or confirmed violations and notifying the appropriate managers if a violation has occurred. Although it is not necessary to inform staff about the actual technology behind the solutions deployed, it is worth explaining their top-level capabilities.

**This is an example only. You should seek formal legal guidance when developing your own AUP.*

- **Gateway email protection**. Commonly deployed to block spam and malicious emails from entering networks, gateway protection is highly effective at stopping suspicious or unwanted file attachments, offensive content and sensitive corporate information. The leading solutions scan outbound and inbound messages and attachments, ensuring that no unauthorized content leaves the network. Organizations can choose either to block or quarantine these emails, and administrators are automatically notified of attempted violations.

- **Email server protection**. Security solutions at the email server level protect against the internal circulation of unwanted content. By scanning inter-departmental emails for jokes, photos, chain letters, malware and confidential information which the recipient has no authority to access, organizations can further bolster their email security. As with gateway protection, any violation will be flagged up to the relevant managers.

- **Endpoint protection.** Organizations that permit access to web-based mail over the corporate network should ensure that all endpoint computers – desktops, laptops and mobile devices – are running up-to-date security software. Emails from webmail accounts bypass corporate gateway defences, and so have an unobstructed route into an organization. Endpoint protection closes this loophole by picking up any malicious or unwanted content that employees attempt to download from this source.

> *If employees realize that their messages are reviewed and stored, they might think twice before misusing the email system.*

Procedures for reporting misuse

Employees should be encouraged to report the alleged misuse of email resources and a clear and anonymous procedure must be put in place to facilitate this.

Sanctions for breaching AUP regulations

All users must understand the potential consequences of not complying with the email AUP. These consequences will depend on several factors, including whether the abuser is a first or repeat offender, whether the breach represents illegal, offensive or merely wasteful behavior, the regulatory environment in which the company operates and the firm's cultural outlook. The sanctions will relate to the severity of the offense, ranging from verbal and written warnings, and on to dismissals.

Who is responsible for the AUP?

The HR IT, and legal departments are all stakeholders in the creation and enforcement of an email AUP. Employees should also contribute to an AUP, enabling greater transparency and buy-in and ensuring that everyone is aware of its existence. At some organizations, the CEO or other board members may take an active involvement, as they can be held personally liable for email misuse by any employee. Typically, staff from all three departments should work together to develop the policy, with specific responsibilities divided as follows.

HR role

The HR department owns the overall process of developing an email AUP, taking responsibility for awareness, distribution and training. Using data provided by the IT department, and by responding to reports of alleged misuse, HR conducts audits to ensure that rules are observed, investigates suspected policy contraventions, and implements disciplinary procedures.

IT role

By using the security solution's reporting features, the IT team generates the forensic evidence needed to identify and log email abuse. The data gathered represents the company's principal source of security intelligence, and can be pieced together to analyze each breach and pinpoint the staff responsible. This information can then escalated to HR.

The IT department also advises HR on the changing capabilities of the organization's IT defenses. For example, if a new solution is deployed to scan outbound messages for sensitive material (e.g. credit card or social security numbers), the AUP might need to be amended and email users might require additional training.

Legal role

The in-house or external legal department ensures that the AUP is in line with legal and compliance requirements, and will advise HR to amend it if regulations change.

In cases of extreme abuse, for example, harassment, or the circulation of illegal, libelous, or confidential information, the legal team will play a role in any disciplinary hearing, and can be required to provide evidence to the courts or other external bodies.

The legal department will also sign off the policy, ensuring that any sanctions contained within it are enforceable by law.

Summary

While the threat of spam and malware is usually linked to inbound emails, an organization's own users can often cause just as much or more damage through the emails they send or share. Employees can be responsible for data leakage, the dissemination of inappropriate or offensive content, and consuming bandwidth through the unnecessary sharing of files, each of which represent a considerable threat to the email network. To ensure that employees recognize these risks, organizations should implement a comprehensive email acceptable use policy which, to be effective, requires enterprise-grade security solutions for the gateway, the email server and all endpoint computers.

Sophos solution

Sophos Email Security and Control protects the entire email infrastructure, with a range of products engineered specifically for the needs of business, education and government. It includes both appliance- and software-based solutions for the email gateway, as well as software solutions for email servers.

Sophos Endpoint Security and Control is a multi-platform solution that seamlessly integrates anti-malware with application control and a client firewall. It features an advanced centralized management console for easy administration and deployment. Sophos Endpoint Security and Control also features network access control (NAC) functionality. Sophos NAC Advanced gives you greater control through more sophisticated policy definitions and advanced reporting capabilities.

Sophos Web Security and Control is an appliance-based solution that protects against spyware, adware, viruses, malicious code, unwanted applications and undesirable content on the web. All Sophos solutions deliver superior protection with less administrative effort.

APPENDIX

Acceptable Use Policy for email

1. Overview

The use of email by users is permitted and encouraged when it supports the overall business objectives of [organization name]. This policy defines what [organization name] considers an appropriate and inappropriate use of the email system and sets out what action [organization name] will take in order to ensure and enforce appropriate use.

The overall objectives of this policy are to comply with all applicable laws and industry regulations, to encourage a safe and pleasant working environment for all users, to minimize email service disruptions and to prevent unnecessary strain being placed on [organization name]'s IT resources.

2. Scope

This policy applies to all users – employees, contractors, consultants, temporary staff and other workers – who can gain access to email systems owned by [organization name]. It applies to all equipment owned by [organization name] and covers all email records.

3. Appropriate use of email

a. Email users are expected to check their email accounts and respond to messages on a regular basis.

b. Users should use the email system to send and receive relevant business information which is in line with the responsibilities set out in their job descriptions.

c. Users should use email to communicate with fellow employees, customers, clients, business partners and other key stakeholders of the business.

d. All email correspondence should be courteous and professional, and users should take care to ensure correct spelling and grammar.

e. Users are expected to manage their mailbox by organizing messages and by deleting emails that are no longer required.

f. All emails should include a signature. This should include the sender's email address, telephone number and [organization name]'s web address.

g. All emails should include [organization name]'s approved disclaimer.

h. Personal use of [organization name]'s email system is permitted unless it impacts on the user's ability to fulfil his or her job description, or if it prevents other users from utilizing the email system.

4. Inappropriate use of email

a. Confidential business information must not be emailed outside [organization name]. Neither should it be forwarded to unauthorized departments or unauthorized personnel within [organization name].

b. The use of email for illegal or unlawful purposes, including (but not limited to) fraud, libel, harassment, the spreading of computer malware or obscene/defamatory content, is prohibited.

c. Users must not use email to propagate computer viruses. Users should also not open unsolicited or unexpected file attachments, which often harbor malicious viruses.

d. [organization name]'s email system should not be used for personal business purposes or to broadcast personal opinions on political, religious or other non-business critical matters.

e. Users must not store file attachments in their mailboxes. All files should be stored at the appropriate location on [organization name]'s shared network.

f. Users should not "cc" or "bcc" multiple recipients unless there is a proven need to do so.

g. Users must not store any personal emails or personal files sent via email on their work computer or on [organization name]'s shared network.

h. Users must not access the email system from their own personal computers or email devices, from public computers, or over the public internet or public Wi-Fi networks, unless these devices and networks comply with [organization name]'s IT security specifications.

5. Monitoring and enforcement

[Organization name] has the right to monitor all email messages passing through, or stored within, its email infrastructure, and deploys monitoring technology to ensure all users adhere to this policy. Users should be aware that authorized IT, HR and legal personnel at [organization name], may – from time to time – access user emails. If, as part of this process, non-compliant emails are discovered, these messages will be retrieved and can act as evidence in disciplinary or legal proceedings.

6. Procedure for reporting misuse

Allegations of misuse of [organization name]'s email resources should be immediately reported to [insert name and contact information of designated person in HR]. Users reporting misuse should also provide a copy of the non-compliant message to the above person. Users should not forward the email to any other person, and must not reply to or delete the message.

7. Sanctions for non-compliance with this policy

Failure to comply with this policy will invoke disciplinary procedures. These include warnings (verbal and written), the withdrawal of email access and termination of employment. If appropriate, legal action will also be taken.

Further details of these procedures are provided in [organization name]'s disciplinary code [insert title].

8. Signature

I confirm I have read and understand [organization name]'s Acceptable Use Policy for email.

NAME:

SIGNATURE:

DATE:

Sources

1 www.idc.com

2 *Securing the Enterprise through Network Access Control (NAC) and Data Loss Prevention (DLP), IDC Research web conference, December 20, 2007*

3 www.sophos.com/pressoffice/news/articles/2007/11/data-leakage-poll.html

4 www.radicati.com

Further examples of an email AUP

www.sans.org/resources/policies/Acceptable_Use_Policy.pdf
www.businesslink.gov.uk/bdotg/action/detail?type=RESOURCES&itemId=1074403458&r.s=sl
www.infotech.com/SEM/Policies/SEM_PolicyEmailAccept_1107.aspx

About Sophos

Sophos enables enterprises worldwide to secure and control their IT infrastructure. Our network access control, endpoint, web and email solutions simplify security to provide integrated defenses against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage and compliance drift. With over 20 years of experience, we protect over 100 million users in nearly 150 countries with our reliably engineered security solutions and services. Recognized for our high level of customer satisfaction, we have an enviable history of industry awards, reviews and certifications. Sophos is headquartered in Boston, MA and Oxford, UK.

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

SOPHOS
WWW.SOPHOS.COM