



CLEARSWIFT™

Simplifying content security

Simplifying content security
Ensuring best-practice email and web use

Clearswift White Paper

The Threat Within:

**The dangers of
unrestricted employee
use of corporate IT
systems**



Table of contents

Introduction	3
A classification of internal threats	4
Risk, and cost of protection	4
The cost of internal threats	5
What you can do	6
Clearswift's MIMESweeper range	7
About Clearswift	8

27% of Fortune 500 companies have had to deal with harassment claims concerning email (IDC).

Read the full story:

http://www.cryoserver.com/servlet/dycon/zen/text/cryoserver/cryoserver/en/graphic/netabuse_index

62% of FTSE 1000 companies had employees distributing offensive email.

Read the full story:

<http://www.internet-policy.com/consequences.html>

Five U.S. brokerage firms were fined \$8.25 million for failing to retain and/or produce e-mail according to SEC regulatory guidelines.

Read the full story:

<http://www.sec.gov/news/press/2002-173.htm>

According to the FT, France Telecom accidentally emailed a draft version of its financial results slide presentation to analysts one week early.

Read the full story:

<http://www.ferret.com.au/articles/F1/0C00DE F1.asp>

Dow Chemical fired 50 employees because of pornographic email messages and Borland International filed suit against one of its employees who sent confidential material to a new employer via email.

Read the full story:

http://www.poynerspruill.com/infocenter/Employment_Law/recent_employer_actions_emphasize.asp

Introduction

Conventional wisdom has led us to believe that external security threats - such as spam, viruses, phishing, trojan horses - cause the majority of security incidents.

While this may be true, too few companies are paying sufficient attention to the very significant issue of internal threats. On average, there is eight times as much email sent internally as there is externally. Together with unrestricted web usage, the threat from breaches of security originating from inside the company's firewall can be punitive. Government statistics back this claim up: according to the 2004 DTI's Information Security Breaches Survey (produced by the UK DTI), one third of British businesses say that the source of their worst security incident is internal.

In a recent, Ponemon Institute Survey on Data Security Breaches, sixty-nine percent of organizations reported serious data leaks caused by either malicious employee activities or non-malicious employee error. Most were because of employee error and lax rules about access to confidential information. Here are some of the statistics from the study:

- 39% involved confidential business information
- 27% involved personal information about customers
- 14% involved intellectual property including software source code
- 10% involved personal information about employees

Moreover, one in 25 businesses identified incidents as being caused by a mixture of internal and external agents: examples given included viruses spread by staff action and collusion between staff and outside agents.

A classification of internal threats

The internal threat is magnified by the growth in electronic communications systems. Meta Group, for example, conducted a survey in 2004 among 500 business professionals and 80% of them preferred e-mail over the telephone as a communication channel. The top three reasons cited for choosing e-mail were:

- e-mail leaves a written record;
- e-mail can be sent to multiple parties at one time;
- e-mail communication can occur without the sender and recipient being online simultaneously.

In addition to email, the web is a core business tool for most employees and nearly all office workers. A recent Clearswift Internet Survey of 2500 organizations showed that:

- 71% of companies provide web access to all employees and another
- 28% provide access to some staff
- 65% of companies allow the use of web-based email. Of these, over three quarters allow its use for personal email.

Add to this the use of chat rooms, forums, instant messaging, peer-to-peer and web applications and it becomes clear just how much traffic passes through the HTTP gateway - and right through corporate firewalls. While many companies are obsessive about external email security to protect against external threats, far fewer pay the same attention to the threat capability of internal email and web use.

The first UK email libel trial took place in 1997 when Western Provident (WPA) brought a case against Norwich Union Healthcare (NUH). NUH had been circulating internal emails rumouring that WPA were in severe financial difficulty and were being investigated by the Department of Trade and Industry. The case was finally settled out of court, NUH admitted that there was no truth to the rumour and paid WPA £450 000 in damages and costs.

Read the full story:
http://www.gap.co.uk/news_may00.html

A mobile phone company recently sacked 40 staff for downloading pornographic images from the Internet using company systems and time.

Read the full story:
<http://www.pcdelete.com/stats.htm>

The CEO of Cerner Corporation used e-mail to express his displeasure over employee performance. Disgruntled employees posted the CEO's angry message on Yahoo!, where it was read by employees, as well as financial analysts and investors. Cerner's stock valuation plummeted 22 percent, from \$44 to \$34 per share, in just three days.

Read the full story:
<http://www.smallbusinesscomputing.com/biz/tools/article.php/688301>

Abuse of email and web browsing make up the majority of internal misuse incidents. Large companies are three times as likely to have had incidents as small ones because the more staff you have, the greater the chances of misuse. According to the DTI, one in 12 companies say their worst security incident of the year stemmed from staff misuse of the Internet and roughly 20 per cent of these were seen as having a very serious impact.

Excessive personal email use, access to inappropriate websites, excessive web surfing and staff sending inappropriate email or accessing another person's email account are the key sources of internal threat.

The hazards fall into the following areas:

Regulation and compliance

Companies are now more accountable for how information is stored, used and distributed - so it is imperative that data is managed and controlled correctly.

In the US, new legislation around the privacy of health and medical information enshrined in HIPAA rules, the need for financial and accounting compliance to Sarbanes-Oxley and new SEC controls related to share dealing scandals have raised the cost to business of non-compliance.

In Europe, the Data Protection Act, Basel II, FSA regulations and EU94/96 are acting in the same fashion. All of this legislation forces companies to provide clear audit trails to ensure that email from their employees complies with financial disclosure and privacy regulations.

In the US and Europe, fines for non-compliance are potentially crippling and jail sentences for company directors who fall foul of the law are common. Businesses now have a legal requirement to stop their employees from breaching regulations.

Confidentiality

As email security becomes more common, webmail accounts (such as Hotmail or Yahoo! Mail) are increasingly used to by-pass corporate gateway security in order to send confidential information out of the organization. Without web content security in place, important financial information, strategic plans and new product designs can be lost.

Legal liability

Employers have a duty to protect staff from 'hatemail' and sexual or racial harassment. Failure to do so can result in liability. Companies can also be prosecuted for illegal downloads of pornography, unlicensed software and music and video files.

In addition to the problems in this area, there are increasing numbers of companies whose reputation has been damaged once the improper use of webmail and web applications are made public and covered by the media.

Security

Every organization's IT infrastructure is in danger from malicious code such as viruses, Trojan horses and spyware - all of which are just as readily downloaded or transmitted via webmail and other web applications as they are by traditional email. In a recent Clearswift survey, over 45 per cent of respondents said they regularly accessed their own personal webmail from work.

Viruses, Trojans and malicious code can all be transmitted via internal email and sent to customers and partners. They can also be brought in on disk, via a laptop, used externally and then circulated throughout the company and sent to customers and partners. With the vast majority of internal communications being carried out electronically, the chances of attacks on data integrity are increasing.

Productivity

As employees increasingly rely on email as the main communication vehicle, the volume of emails has grown exponentially. A recent survey by Clearswift showed that over 40 per cent of employees in British, German and US firms spend more than an hour each day on non-work-related emailing sharing jokes and making arrangements with friends. In addition, current trends in advertising encourage employees to manage personal business (e.g. bank accounts, insurance etc.) via the web.

This means that in a typical 100 person company, in each of the three countries, almost 1700 working days each year are lost because people are using corporate email systems for non-company purposes, the equivalent of seven new full-time staff.

In the same survey up to 10 per cent of employees said that they regularly download pirate software - music, films, games or applications - while at work. And almost four per cent - one in 25 - said they responded to spam offers via the corporate email system. Spam is the main source of malware.

The cost of internal threats

The cost of these internal threats can be devastating. According to Techweb, for example, British companies alone could be losing up to £30 billion each year in wasted employee time and productivity. The newswire identifies eBay, travel sites, car-shopping, price comparison, banking, stock-watch, cyber-dating and pornography as the main time eaters. The BBC has said that any company that could cut this time wasting could profits jump by up to 15%.

The potential costs of internal threats are not simply linked to productivity issues. They also include:

- **Downtime** - Viruses, trojans and malicious code that bring down systems can originate or be propagated within the company.
- **Reputation damage** - Your customers and partners won't thank you for exporting malware that damages their systems or offensive content that leaves them liable.
- **IT resource drain** - Bandwidth and storage cost money. Don't waste it on email that is malicious, uninvited or frivolous.
- **Legal liability** - Your company is vulnerable to litigation caused by the internal or external circulation of offensive content or copyrighted material.
- **Breach of confidentiality** - The circulation of confidential information can seriously affect your ability to compete. Confidential documents can also be circulated to the wrong people or departments inside the company.
- **Compliance breaches** - New regulations make your company accountable for how data is stored, used and distributed. Manage it or you're in violation.

What you can do

A key issue here is that most significant companies have content security defences in place to handle the email threat. But these only counter the inbound threat from viruses and spam and the like. Business must realise that gateway security is simply not enough to protect your organization from the plethora of internal threats. There are three steps.

1. Put a policy in place

Internal email and web security is at heart a policy issue. Each organization has to decide how it wants its employees to use email and the web, which activities are allowed by whom and which are forbidden.

No two organizations will have the same policy because no two organizations do business in the same way. An internal security policy will reflect both the nature of the business and the organization's culture. For example:

- Some organizations prohibit all non-business surfing while others allow it at lunchtime and after 5:00pm.
- Some block webmail, others allow it and still others only let certain departments use it.
- Some organizations block the sending out of all attachments, some block spreadsheets, others block CAD designs.

Whatever decisions are made, no security technology can do its job unless it's referencing a clear set of policies.

2. Communicate the policy

The point of internal security is not to catch as many rule-breakers as possible. It is to educate all employees, to remove temptation and deter breaches of policy.

The best security policy can only be effective if all staff are aware of it. Once a policy is in place (along with the technology to police it), it's essential to make sure that all staff are clear about the policy and understand how it is being monitored and managed. This should include a module in new employee induction programs that explains the policy and shows how it is being implemented.

3. Implement multi-layer content security

Once a policy is in place, it must be enforced and monitored using multi-layer content security. Firewalls, user authentication and intrusion detection are core infrastructure security tools, but they only have 'block/allow functionality and SMTP and HTTP always fall in the allowed category. Anti-virus software protects against viruses, but can only react to known threats.

Address Lookup is software designed to block access to traffic deemed a threat to company security according to a database of blacklisted addresses. This is an important first line of defence. But effective email blocking and URL filtering must cover a huge range of addresses in many categories and languages to be effective. It may help to ensure these lists are automatically updated and allow granular policy support so that rules can be set for individual, department, time of day and type of traffic.

Complete Security comes from being able to conduct content analysis by providing software that scans content in real-time according to policy. This will permit or deny access depending on analysis of file type, text, images and embedded code.

The data in the email message transfer is analyzed and evaluated in line with the organization's security policy, depending on sender-recipient route. Emails can be blocked based on file types, inappropriate text or offensive images.

This multi-layer approach to web content security is the only way to block every kind of threat to the network and the business, whether incoming or outgoing. Organizations serious about protecting themselves from internal threats should settle for nothing less.

Clearswift's MIMESweeper range

Email security, simplified

The MIMESweeper portfolio

Clearswift's MIMESweeper family of email security products includes comprehensive solutions for inbound, outbound and internal email.

The solutions combine anti-virus and anti-spam with the award-winning MIMESweeper content filtering engine. Optional archiving and TLS encryption complete the unified security solution.

All MIMESweeper email solutions simplify the deployment, management and maintenance of the entire content security activity, with intuitive management and reporting consoles, automatic updates and personal message management.

EAL4 accredited solutions for government, defense and financial sectors

Clearswift provides a range of security solutions, accredited to EAL4 standard, for highly sensitive government, defense and financial institutions. Products such as Bastion™ and DeepSecure™ address the security needs of the world's most mission-critical messaging applications for clients such as the UK Ministry of Defence and NATO.

Web security, simplified

The MIMESweeper family of web security solutions does for HTTP web traffic what the email products do for SMTP: analyze every bit of traffic and remove every kind of content threat.

For the first time, enterprise can defend against spyware, web-borne viruses, loss of confidential information, prohibited browsing, illegal downloads & uploads with just one solution.

The MIMESweeper web solutions combine the world-class content analysis technology of MIMESweeper with a powerful URL Filter and world-leading anti-spyware.

Three different deployment platforms

Clearswift is the only vendor to offer complete content security solution in all three delivery platforms: as software, on an appliance or as a managed service:

- **The MIMESweeper software** family includes comprehensive content security solutions for corporate email (inbound and outbound), internal email, web traffic and webmail.
- **The MIMESweeper appliances** deliver complete content security in a plug 'n' play appliance for rapid deployment and easy management.
- **The MIMESweeper managed services** deliver full content security as hosted services to stop email- and web-borne threats before they even reach corporate servers.

About Clearswift

Clearswift simplifies content security. Our products help organizations enforce best-practice email and web use, ensuring all traffic complies with

internal policy and external regulations. Our range of content filtering solutions makes it easy to deploy, manage and maintain no-compromise email and web security for both inbound and outbound traffic.

Clearswift is the only vendor to offer comprehensive, policy-based content security in all three deployment methods: as software, as an appliance and as a managed service. All three platforms are designed to take the hassle out of securing internet traffic, with a clear, intuitive management interface; automatic, 'zero-touch' updates; powerful reporting and common-sense policy management.

Twenty years of experience across 17,000 organizations has helped us raise security standards while simplifying security management at the same time. We've helped many of the world's most successful organizations use the internet with confidence and are committed to staying ahead of the market and helping our customers defend against all emerging threats.

Contact Clearswift

United States

100 Marine Parkway, Suite 550
Redwood City, CA 94065
Tel: +1 800 982 6109 | Fax: +1 888-888-6884

United Kingdom

1310 Waterside, Arlington Business Park, Theale,
Reading, Berkshire, RG7 4SA
Tel: +44 (0) 11 8903 8903 | Fax: +44 (0) 11 8903 9000

Germany

Amsinckstrasse 67, 20097 Hamburg
Tel: +49 40 23 999 0 | Fax: +49 40 23 999 100

Australia

Ground Floor, 165 Walker Street, North Sydney,
New South Wales, 2060
Tel: +61 2 9424 1200 | Fax: +61 2 9424 1201

Japan

Hanai Bldg. 7F, 1-2-9, Shiba Kouen Minato-ku
Tokyo 105-0011
Tel: +81 (3) 5777 2248 | Fax: +81 (3) 5777 2249