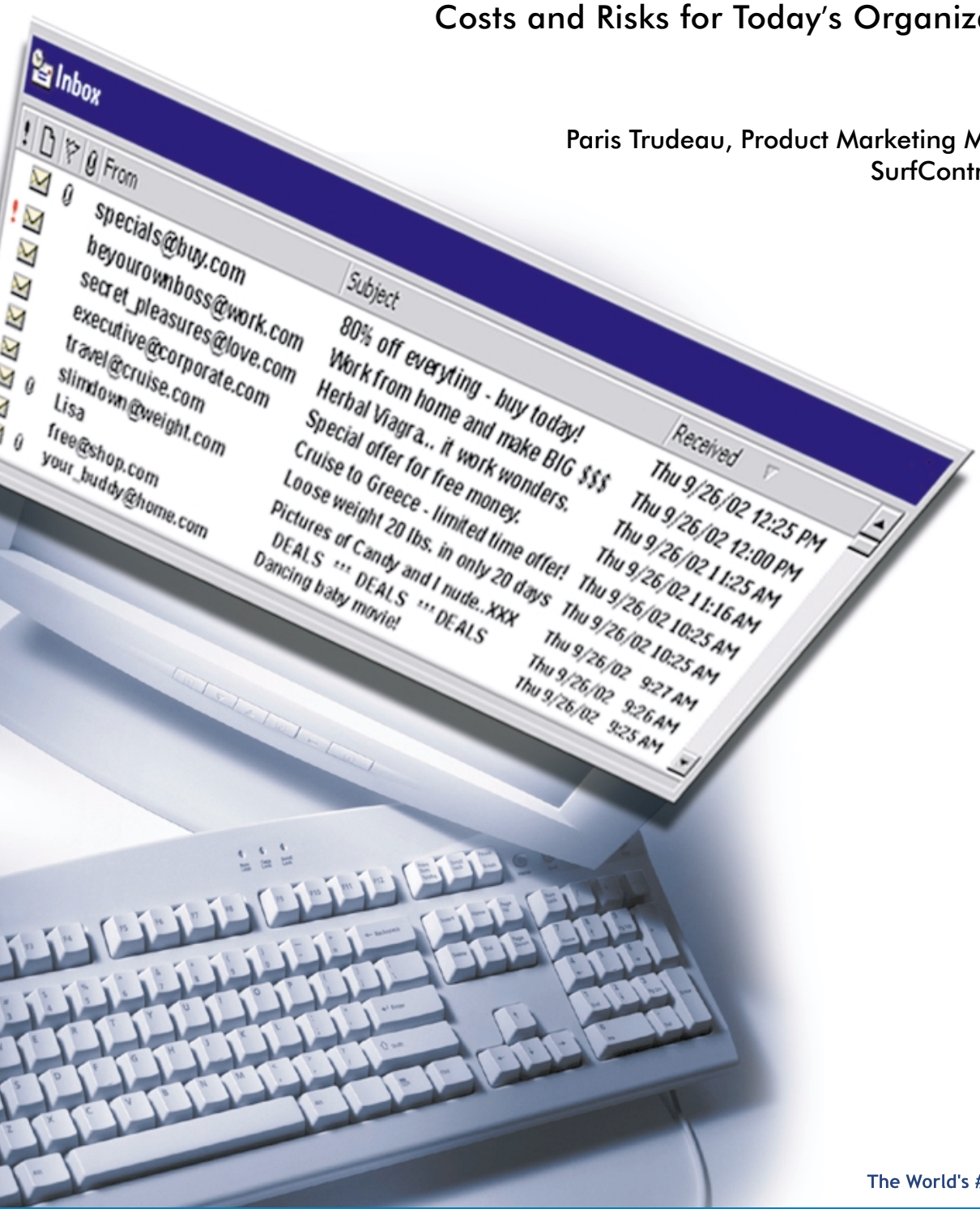
Fighting the New Face of **Spam**

The Rising Tide of Spam Means a Flood of Costs and Risks for Today's Organization

Paris Trudeau, Product Marketing Manger
SurfControl Inc.



SurfControl®
The World's #1 Web & E-mail Filtering Company

Contents page no:

Introduction

Spam, or junk e-mail, is on the rise again, clogging the arteries of networks and servers and sending the blood pressure of many administrators through the ceiling.

And while the scourge of spam has taken a back seat to threats from viruses and hackers in the past, many organizations are now recognizing their vulnerability to the risk of spam and reassessing their response.

Despite the threat of tougher legislation and stiffer financial penalties, the cost of spam to the enterprise continues to rise. More ingenious spamming methods, combined with an increasing use of e-mail in the workplace, have dramatically increased the volume and variety of spam that needs to be managed daily.

As organizations around the world look for an effective solution, new kinds of junk e-mail threats have emerged that can be just as costly as their traditional counterparts. Junk e-mail sent to the workplace by well-meaning family and friends can have the same harmful effect on network bandwidth, user productivity, and legal vulnerability as the most professionally orchestrated commercial spam campaign.

To fight this well-meaning menace, organizations need to understand how spam is evolving. With this spam evolution, they must also change their response to it and look to more powerful and sophisticated technologies for a solution.

The Rising Tide of Spam

As the use of e-mail has exploded around the world, for personal and business use, so too has the scourge of spam.

In the early days of the Internet spam was widely considered as just another unavoidable cost of a well-connected world. But as the Internet has grown, and users grown more dependent upon it, spam has risen to the status of a global epidemic. Internet research company Jupiter Media Metrix predicts users will receive about 206 billion junk e-mailings by 2006.

So costly and risky has the threat become it has not only created an entire business focused on fighting spam, it has forced governments around the world to take action against spammers.

Governments have been forced to try and cope with this growing menace on behalf of the public. However, because of the no-borders nature of spam, governmental regulation seems to be a difficult way to solve the problem since no world government exists to police the matter.

A mixture of anecdotal evidence and hard research offers some clues to how bad the spam problem really is. According to research firm IDC, by 2005 the number of e-mails exchanged every day will exceed 36 billion worldwide. Estimates for the percentage of e-mail messages that can be classified as spam are approximately 40%.

"There is a genuine concern that too much spam will kill off e-mail."

Eric Allman
Creator of the world's first Internet mail program

Even conservative estimates suggest than in the next couple of years Internet users will be sending and receiving more than 10 billion spam messages each day. That's 10 billion additional messages that will decrease user productivity, overload servers, and reduce many networks to a crawl.

This conservative estimate is backed up by industry claims in a recent ZDNET news report of nearly 5 million spam attacks this year alone. Given that each attack can consist of millions of individual e-mail messages, it's easy to see why the problem has been described as epidemic.

Recent research supports the belief that the problem of spam will get worse before it gets better, with a number of organizations reporting a five-fold increase in spam attacks in just the last year. So bad has the problem become, one of the earliest e-mail innovators believes it could threaten the very viability of e-mail.

In an interview with Silicon.com, e-mail pioneer Eric Allman commented, "There is a genuine concern that too much spam will kill off e-mail. We haven't quite got there yet, but it could happen." Mr. Allman wrote one of the world's first and most popular Internet mail programs in 1981.

And no organization or nation is immune. According to CNN, Hotmail has to deal with more than 1 billion pieces of junk e-mail sent through its servers each year. This is a common problem for many ISPs and e-mail providers, who usually have little choice but to pass the cost on to the customer.

A report in July 2002 found that more than 15% of e-mail received by U.K. firms each day is spam. And in May 2002, the Korea Times reported that unsolicited e-mail costs Korean Internet users and ISPs $2.25 billion a year. In just one day, nearly 900 million spam e-mails were sent to

Korean e-mail subscribers, while the number of spam e-mail circulating in that country now exceeds 340 billion messages annually. That's around 21 spam e-mails every single day for every man, woman, and child in Korea.

According to the Congress Online Project, the number of e-mails sent to the U.S. Congress has more than doubled in the last two years, with some senators receiving as many as 55,000 e-mail messages each month.

The Federal Trade Commission receives 15,000 spam complaints every day, and with spam on the rise, organizations are seeing their networks overwhelmed and productivity decline.

Last year alone, Congress received a total of 80 million messages. There's no estimate for the number of e-mails that were spam because their e-mail servers were so overloaded they simply had to ignore the good with the bad. But if current trends are anything to go by, as many as 24 million of those messages were spam.

Spam now ranks with viruses and hackers as one of the costliest threats to organizations worldwide, and most of that cost is felt in the workplace.

The Changing Face of Spam

Spam comes in all shapes, sizes, and flavors, and not all spam can be simply defined by the current statutes or common understanding. While much of the spam circulating across the Internet comes from the traditional sources, it is a mistake to assume that there's only one kind.

Unsolicited Commercial or Bulk E-mail

The most notorious brand of spam is the most common – the unsolicited bulk e-mail distributed by the millions and featuring everything from health and investment schemes to work-at-home opportunities and chain letters.

In an effort to ensure maximum response and effectiveness, spammers are becoming more creative in the way they create and distribute the messages, hoping

"A company with 10,000 employees loses more than $13 million worth of productivity each year because of in-company spam."

Gartner

to dupe even the more cautious recipient and at the same time, skirt the victim organization's strict legal guidelines.

The Family-and-Friends Assault

A new form of spam is taking its toll on networks. Described by research firm Gartner as "friendly fire," the amount of e-mail sent to employees by their family and friends is on the increase. As users become more familiar and comfortable with creating and sending graphic images, these e-mails are increasingly made up of bandwidth-hogging files including MPEGs, gifs, BMPs and mp3s.

As a result, many workplaces are inundated with unnecessary personal e-mails with large attachments. These include family photos, home videos, cartoons, jokes, electronic greetings and a host of other electronic files. Although the senders mean well, the employer's networks and servers pay the price. Not to mention any loss in productivity as employees view and forward these files.

According to a survey conducted by Market Facts' e.Nation, every single week employees receive up to 30 chain letters, jokes, video clips or similar junk e-mail messages from someone they know. This means many American workers have to deal with more than 1,500 pieces of junk e-mail each year from friends, family and colleagues. This also means that traditional spam, the much-reviled commercial e-mail sent by strangers, won't even reach the proportion of "friendly" junk e-mail until 2006. Internet research firm Jupiter Media Metrix predicts that by 2006 consumers will be receiving an average of 1,400 pieces of commercial spam each year.

Little do these well-meaning friends know that sending just one 5-megabyte joke screen saver takes up the same amount of space on a company server as 160 plain text e-mails.

Jupiter Media Metrix estimates that each piece of unwanted e-mail costs companies $1 in lost productivity. Using this calculation, friendly junk e-mail could cost a company with 500 employees nearly $750,000 each year.

This burden can jump when employees forward personal electronic files to large groups of co-workers. It's easy to understand why an employee might want the entire organization to see a sixty-second video of a daughter's wedding, but it's equally easy to understand the frustration IT administrators feel when this is a daily, if not hourly occurrence.

And there's more to the problem than mere irritation. According to Gartner, a company with 10,000 employees loses more than $13 million worth of productivity each year because of spam internally generated and distributed.

The Many Costs and Risks of Spam

The early spammers defended their business practices by arguing that spam had no victims, and that the only cost involved was the effort it took to hit the Delete key. While that argument had little credibility then, it has absolutely none today.

In the workplace, spam can have a huge effect on user productivity, network resources, legal liability and network security.

The Impact on User Productivity

Spam could be costing millions of dollars each year in lost productivity alone.

According to Ferris Research, the average employee wastes $4,000 each year dealing with e-mail. That's based on the assumption that an average of 115 hours is spent by an employee each year managing the contents of their inbox - reading it, responding to it, deleting it and so on.

The report calculated that the average hourly cost of an American worker is $35, so assuming that a third of this effort is devoted to dealing with spam, that amounts to more than $130 billion annually in wasted productivity for America's 100 million+ workforce.

"10 percent of U.S. employers have been subpoenaed to produce employee e-mails in lawsuits."

IDC

The Impact on Networks and Servers

The Richard Ivey School of Business in London, Ontario, estimates that the average North American worker now gets almost 50 e-mails a day, up 33% from last year.

If we assume that just a third of these e-mails are unsolicited, an organization with 10,000 e-mail users will receive around 150,000 unsolicited e-mails every day. Somebody, or something, has to deal with those e-mails. And that's typically the networks and servers that manage and distribute e-mail within the organization.

In May 2002, Network World magazine reported how an avalanche of 15,000 spam e-mails took down a midlevel SMTP gateway server at a major credit information company, bringing e-mail to a grinding halt for 10,000 end users in 35 countries.

Even though spam is effectively blocked by the right kind of filtering, some e-mail registered as borderline and isolated for inspection still has to be inspected. That takes manpower. When spam arrives at the user's desktop, simply deleting it does not delete the problem. As spam that is backed up on archiving systems on a daily basis can consume valuable bandwidth if it isn't filtered from delivery, that spam will still take up valuable storage space until the organization purges its Deleted Files folders.

The Legal Risks

Unfiltered spam can also create enormous legal risks for both employers and employees. Despite warnings and policies, many employees continue to exchange adult, racist, hate and other offensive material in the workplace, often creating resentment amongst co-workers, and triggering harassment lawsuits.

A 2001 study by research firm IDG found that 10 percent of U.S. employers have been subpoenaed to produce employee e-mails in lawsuits. And according to the ePolicy Institute, 8 percent of firms have had to deal with sexual harassment or discrimination claims because of inappropriate use of e-mail and the Internet by employees.

When spam received in the workplace contains offensive content, it creates additional legal risks. Employees who forward chain letters, special offers, investment schemes and other misleading e-mails to co-workers risk creating liability for the employer. Employees are essentially spokespeople for their company, sending junk messages on electronic company letterhead.

And if an employee receives unsolicited commercial e-mail that they find offensive (such as adult content), they could hold their employer legally responsible. To make matters worse, if an employee forwards a joke or personal "friends and family" junk e-mail, they put their employer at risk if someone who receives it outside of the company is offended by its content.

The Security Risks

Apart from the loss in productivity when employees have to deal with spam, there can be additional network security risks to an organization with the introduction of viruses and malicious code being delivered through spam messages.

Spammers use the temptation of an irresistible offer to lure recipients into opening an e-mail or attachment they would normally treat with greater caution, and giving in to that temptation can often be the first step in a very costly virus outbreak.

Spam as Scams

Recognizing that most spam today promotes some form of scam, the Federal Trade Commission (FTC) has taken an active role in protecting businesses and consumers from the dangers of spam.

In 1998, the Commission set up a special mailbox to collect and investigate spam, receiving nearly 4,000 spam e-mails a day in the first year. Three years later the same mailbox was receiving 40,000 spam e-mails every day, a ten-fold increase in just 36 months.

The Commission noticed that much of this spam was a scam – frauds, cons, and schemes designed to lure the recipient into a scam. That growth was one of the reasons that prompted the FTC to regularly issue its Dirty Dozen – a list of the top 12 spam scams. These scams include almost every conceivable type of fraud including business opportunities, bulk e-mail, chain letters, work-at-home schemes, health and diet scams and investment opportunities. To find a detailed list and description of the top 12 spam scams visit www.ftc.gov/spam.

The Weakness of Traditional Countermeasures

Traditional spam filters have been the backbone of the spam counter-offensive for years, almost maintaining spam traffic to a manageable level and keeping much of it from entering the workplace.

But traditional or less sophisticated technologies remain weak against modern threats, and many of today's most popular spam fighting solutions are having little effect on the new face of spam.

Most traditional technologies are based on recognizing the tell-tale signatures of popular spam messages. Known as origin and lexical filtering, they rely on either recognizing the domain name or IP address of the sender as being that of a spammer, or on recognizing the content of the message as being spam.

For example, subject lines like “Hot Investment Opportunity” and “Lose 20 lbs in 10 Days,” known as “tip-offs,” have always been easy to spot and block without much intelligence on the part of the filtering technology. This is a typical example of “lexical filtering” - recognizing known key words or phrases.

Origin-filtering solutions rely on the use of blacklists (also known as hot lists or “not-lists”) to block e-mail from addresses known to be used by spammers. And while that method has had some success, its effectiveness is limited. Spammers are able to get around blacklists by routing the spam through legitimate free e-mail accounts like Hotmail. And black listing is always a response after the event - a spammer’s address is only added to a blacklist after the spammer has used it.

There’s also the growing problem of false positives - legitimate e-mail often falling victim either because the e-mail address looks similar to a “key” address, or because someone disgruntled with the sender added their legitimate address to a blacklist database.

Spammers have also become more resourceful in their strategies, routing their messages through a myriad of servers and addresses in an attempt to clean the point of origin from its hot status, faking their addresses, or using the e-mail addresses of legitimate and unsuspecting e-mail users. They can also simply change tip-off subject lines like “Make Millions Working From Home” to more obscure headings like “Here’s the information you asked for.”

Even basic keyword filtering that relies on the recognition of specified keywords to block spam has its weakness. For example, a filter that blocks any e-mail with the word “sex” in it could also block an e-mail with a more innocent word like “sextant.” In the United Kingdom many cities and counties end in the word sex (like Essex, Sussex, and Middlesex) so the potential for false positives is significant with basic keyword filtering.

Weaknesses like this clearly demonstrate that more powerful technologies are needed so that filtering does not have to be backed up by time-consuming human intervention to ensure filtering is accurate, up-to-date, and effective.

A More Intelligent Response to Spam

New filtering technologies must look beyond the limitations of blacklists and basic keyword scanning, and look for solutions that don’t rely solely on recognizing IP addresses that can be easily changed or forged.

Spammers can take many steps to hide their identity, but faking the content of their message is self-defeating. The recipient simply won't be able to understand the message. This is the spammer's Achilles' heel.

For effective anti-spam defense, organizations must implement a layered security strategy. Only SurfControl offers multiple layers of anti-spam protection:

1) Anti-Spam Agent

SurfControl's Anti-Spam Agent is a powerful tool that compares incoming e-mails with a database of classified spam and junk e-mail content - letting administrators decide which e-mails to restrict or allow.

It is the only spam-filtering database capable of classifying known spam content into different categories, such as "Adult," "Hoax/Rumor," "Illegal Material," and "Chain Letter." It can even further classify content by media type, such as text, graphics, and executable.

These features give administrators the ability to specify exactly how they want e-mail in each category to be handled - delayed, isolated, deleted, or even allowed. Anti-Spam Agent scans both the e-mail and any attachments, including JPEGs, GIFs, and MPEGs.

Anti-Spam Agent's unique digital signature filtering is highly accurate and efficient at reducing time and resources required to review false triggers.

2) Threshold Scanning

SurfControl E-mail Filter comes equipped with 15 pre-defined content dictionaries classified by categories such as "Spam," "Adult," or "Hate Speech." This gives organizations the ability to specify exactly how they want e-mail in each category to be handled – whether they want it delayed, isolated, deleted or even allowed. Threshold scanning uses a mathematical threshold algorithm.

3) LexiMatch

SurfControl E-mail Filter's LexiMatch feature provides context sensitive language analysis using advanced Boolean, making content filtering accurate and easy to deploy. Pre-defined dictionaries can be used in order to create true content understanding by defining the word association and phrase relationships.

4) Virtual Learning Agent (VLA)

The Virtual Learning Agent (VLA) is a unique content development tool that can be trained to understand and recognize an organization's specific proprietary content. A patented technology known as Adaptive Reasoning Technology (ART) is behind the VLA. SurfControl has used this advanced technology for a number of years to apply the power and flexibility of neural networks to the challenge of filtering. VLA is a neural network engine that is pre-trained on the Adult category – 30% of spam is estimated to be Adult in nature – among other categories. The VLA can also be pointed to a repository of the customer's spam messages in order to build an extremely accurate neural network that will recognize that type of message in the future.

Adaptive Reasoning Technology (ART) is based on four fundamental principles:

- Any kind of filtering must have the intelligence to know what it's supposed to be looking for.
- This intelligence must also include the ability to learn as it works, in order to keep up with changes in spamming strategies.
- Effective filtering must focus on and understand message content, and not just rely on recognizing the sender's address.
- The filter should be able to automatically categorize spam under specific headings to make it easier to verify and validate as unsuitable.

5) HTML Stripper

SurfControl E-mail Filter can be set to strip HTML out of e-mail message. People like to e-mail jokes, chain letters and other such seemingly harmless content to friends, family and colleagues in HTML format. That's why spammers and virus authors often embed malicious code in amusing, compelling and innocent looking e-mail messages. These email messages have active components that can automatically launch these malicious threats simply by taking advantage of the HTML structure of the e-mail.

6) Reverse Client DNS Lookup

SurfControl E-mail Filter verifies that the sender of each message actually exists by using the reverse DNS lookup feature. As people get more clever about avoiding spam, spammers are getting more sophisticated to avoid detection. For example, spammers are now disguising their e-mail addresses to look legitimate. With SurfControl's reverse DNS lookup, companies can block messages if the sender domain doesn't match the DNS domain.

7) Explicit Deny List

With SurfControl E-mail Filter, customers have the ability to create their own deny list of know spammers IP, e-mail and/or domains.

8) Real Time Black Lists

These are the traditional countermeasures for spam that focus on the known spammers from mailabuse.com or other real time black list providers. SurfControl E-mail Filter allows for a real time lookup of any real time black list provider.

SurfControl's continuing research in this area has contributed to its leadership in the global Web and e-mail filtering market.

The New Frontier in Anti-Spam Defense

Just like cybercrime, it is unlikely there will ever be a total cure for spam. Current technologies have won some of the battles against spam, but new technologies can win the war and eradicate spam from the workplace.

Professional spammers will continue to look for ways to evade obstacles. Internal e-mail policies cannot reasonably be enforced on the families and friends of employees. And completely banning the exchange of non-work related e-mails by employees could foster an atmosphere of resentment. But every organization must find an effective way to communicate their Acceptable-Use polices so that every employee understands the true impact that unacceptable use of e-mail has on their workplace.

As professional spammers look for ways to evade obstacles, organizations need to protect themselves with advanced technologies.

Security experts have identified three approaches that are key to the fight against the new face of spam:

Policy – every organization must clearly define its policy towards spam, and effectively enforce that policy.

Education and awareness – every employee must be compelled to comply with this policy. They must also be educated about the harm spam can do the workplace, how their behavior may actually contribute to the problem, and how they can change that behavior to reduce the risk.

Intelligent technologies – organizations must look beyond “origin recognition” and blacklist-based solutions, to a more layered approach to spam protection using intelligent technologies that are a better match for creative spammers.

Newer technologies hold the key. In particular, anti-spam technologies that go beyond simply recognizing text-based junk e-mail to isolate and neutralize bandwidth-hungry spam loaded down with graphics, movies, and music. And technologies that have the intelligence to quickly and accurately separate spam from legitimate e-mail without slowing network traffic even more.

These technologies are available today, thanks to the research at companies like SurfControl. Properly deployed, new approaches to spam management can help eradicate the spam epidemic from the workplace – freeing up networks to focus on the flow of legitimate traffic, freeing up employees to focus on more productive use of e-mail resources, and limiting legal liabilities.

Anti-Spam Tips for Network Administrators

A recent SurfControl survey of more than 700 IT professionals found that more than 90% of organizations provide “basic” to “no” employee training in managing spam and junk mail. Additionally, more than 80% of respondents find that supervisors and junior members of staff are the biggest abusers of company e-mail. In order to help manage the spam issues within an organization, SurfControl recommends these tips for network administrators:

1) Tell users never to respond to spam e-mail messages. Sending a reply, even if it's a request to be taken off a list, confirms a user at an address and encourages the spammer to send more mail.

2) Tell employees not to forward on junk e-mail messages to other coworkers.

3) Include guidance in your Acceptable Use Policy forbidding employee use of their company e-mail addresses when surfing or shopping online.

4) Subscribe to "real time black hole" list services that block delivery of e-mails from known spammers.

5) Subscribe to a Signature Database List, like SurfControl E-mail Filter's unique Anti-Spam Agent, which prevents the delivery of known spam and other digital junk. And make sure you update the subscription list regularly to ensure the most complete protection.

6) Install content filtering tools that scan and block e-mail messages that include suspect text like 'Get Rich Quick' or similar subject words and phrases, and those with multiple forwards or huge distribution lists.