

WHITE PAPER

Messaging Security: A Holistic View of Antispam, Antivirus, Policy Enforcement, and Regulatory Compliance

Sponsored by: Clearswift

Brian E. Burke

October 2004

IDC OPINION

The challenge of controlling electronic communications as they flow into and out of an organization is becoming increasingly more critical. This paper provides line-of-business managers, financial and security auditors, and IT executives with a deeper, more comprehensive view of messaging security. It offers a realistic view of the critical ingredients for optimizing security, preventing spam, and enforcing privacy and regulation compliance across the enterprise-messaging environment. It also outlines the true cost of spam and the value of antispam solutions as well as the impact of privacy and regulation risks on individual industries.

Messaging security products have assumed responsibility for ensuring that:

- Business communications comply with applicable rules and regulations, for example, patient and client data remains private to the client (Health Insurance Portability and Accountability Act [HIPAA] and Gramm-Leach-Bliley compliance), quiet periods remain quiet (SEC compliance)
- Nonbusiness content, such as Spam, doesn't slow down worker productivity, expose the corporation to legal liability, and use up needed bandwidth
- Offensive content, such as pornography or hate material, remains outside the organization
- Inadvertent or deliberate release of corporate confidential information and private customer data gets detected and thwarted
- Sensitive communications receive appropriate encryption and end-to-end protection
- Effective retention and retrieval of mission-critical communications relevant to the requirements of the business ensures that this information is kept for up to seven years

METHODOLOGY

To gain insights into the email management challenges facing enterprises and to learn more about how leading organizations address these challenges, IDC conducted in-depth interviews with IT executives at companies in several industry

sectors. These organizations operate in financial services, manufacturing, insurance, and government agencies. To meet the need for spam-related market analysis, IDC recently interviewed more than 1,000 mid- to upper-level managers to determine the cost of spam and the value of antispam solutions. In addition, IDC met with the Clearswift team to review its goals and tactics. This white paper takes into consideration all of these research perspectives to shed light on the real-world challenges and solutions of email management.

THREATS ON THE EFFECTIVENESS OF EMAIL

Spam

The convenience and efficiency of electronic mail has been dramatically reduced by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Spam has become more than just a nuisance; it is quickly becoming both a major productivity drain and potential legal liability in organizations across the globe. Spam fills networks, servers, and inboxes with unwanted and often offensive content. The business impact of spam only grows more serious as the volume of spam continues to rise.

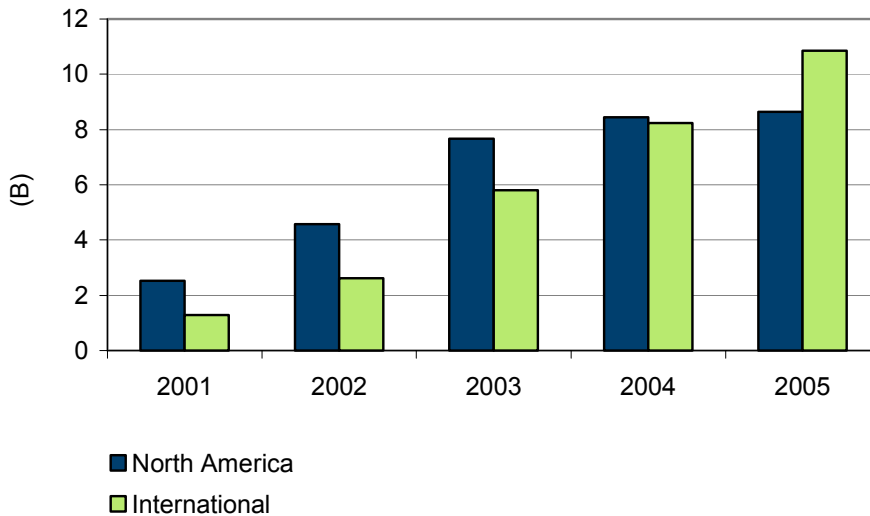
The convenience and efficiency of electronic mail has been dramatically reduced by the extremely rapid growth in the volume of unsolicited commercial electronic mail.

Spam has been a major problem for service providers for several years. However, for most organizations, it has only recently emerged as a high-priority problem requiring high-priority attention and resources. Prior to 2002, companies and other organizations considered spam more of a nuisance than anything else. They considered the volumes of spam received to be manageable through the use of the Delete key, simple keyword email filters to delete or folder suspected spam, and real-time black hole lists (RBLs) to block known sources of spam. Corporate IT departments were too busy with other projects, including battling viruses and other malicious code capable of bringing down entire networks and damaging servers and personal computers, to invest time and money in fighting spam.

What a difference two years make. The volume of spam sent worldwide every day will jump from 7 billion in 2002 to 23 billion in 2004, according to IDC estimates. Spam has grown into too difficult and costly a problem for most IT departments to ignore or leave to email users. Fighting spam can be very time consuming and is best handled by experts who spend all of their time and resources focused on developing even more effective ways to block it. Moreover, spam will contain more non-English language content because the majority of spam will be sent to email users outside North America by 2005 (see Figure 1).

FIGURE 1 (USE NEW FIGURE)

North America and International Spam Messages Sent Daily, 2001–2005



Source: *Worldwide Email Usage 2004–2008 Forecast: Spam Today, Other Content Tomorrow*, IDC #31782, August 2004

The Business Impact of Spam

To measure the cost of spam and the value of antispam solutions, IDC surveyed 1,000 LOB and IT managers representing organizations of various sizes and industries in North America in fall 2003. IDC also interviewed 30 senior IT executives at organizations with more than 1,000 employees in various industries. This section discusses those findings and focuses on spam as part of a larger secure messaging solution.

According to the organizations surveyed, the biggest benefits of antispam solutions are in higher worker productivity (see Table 1). Please note that because the following cost-savings estimates are based on averages of the firms surveyed as well as other information and assumptions about antispam solutions in the aggregate, actual cost savings may vary.

TABLE 1**Average Productivity Cost of Spam and Savings of Antispam Solutions for Firm with 5,000 Email Users**

Workforce Segment	Description	Without Antispam Solution	With Antispam Solution
Email users	Daily time spent by each user	10 minutes	5 minutes
	Average annual (cost)/savings to firm	\$4.1 million	\$783,000
IT staff	Daily time spent by each user	43 minutes	19 minutes
	Average annual (cost)/savings to firm	\$85,800	\$13,000

Source: IDC's Spam Study, 2003

Email Users

Antispam solutions reduce to 5 minutes (a 50% reduction) the average amount of time lost by email users each day due to spam. This translates into a total of \$783,000 in email user productivity gains each year for the 5,000-email-user firm described above. Note that having an antispam solution does not entirely eliminate the time email users spend dealing with spam because of the spam that avoids detection and reaches email inboxes and the fact that organizations choose solutions that involve email users reviewing suspected spam before deletion.

Corporate IT Staff

Antispam solutions reduce the average amount of time lost due to spam each day for corporate IT staffers down to 19 minutes, a 56% reduction. This translates into a total of \$13,000 in IT staff productivity gains from reduction in time spent dealing with spam and viruses carried by spam for the 5,000-email-user firm described above. Note that even after an antispam solution is deployed, there may continue to be a fair amount of spam-related work for IT staffers to do, such as administering servers, updating spam patterns and software, and responding to email users about spam that evaded detection and false positives (legitimate emails incorrectly identified as spam).

Other Benefits

Other benefits from antispam solutions include reductions in network and storage costs, which will vary depending on whether spams are deleted immediately or saved in spam folders for email users to review. Corporate liability for offensive spam content and harm to corporate reputations for relaying spam unknowingly will decrease due to less spam being delivered and the organizations ability to demonstrate steps taken to block spam.

Regulatory Compliance

Legislated requirements for communication security, privacy, and, legitimacy/non-repudiation of the transmission further heighten the importance of securing enterprise's email environments. Organizations are rapidly adapting not only to traditional oversight agencies such as state insurance regulators, rating agencies, securities trading organizations (e.g., the National Association of Securities Dealers), but also, and increasingly, national legislation. This patchwork of legislation covers healthcare privacy (HIPAA), financial privacy (GLBA), corporate governance and accountability (Sarbanes-Oxley), and homeland defense (Patriot Act).

Legislated requirements for communication security, privacy, and, legitimacy/non-repudiation of the transmission further heighten the importance of securing enterprise's email environments

These regulations have caused unprecedented pressure on corporations of various industries to secure the use of their electronic communications, as shown in Figure 2. Many organizations are faced with the complex task of complying with various regulations and making sure that employees do not inadvertently, or deliberately, break the law. Each of these regulations can carry criminal penalties and/or civil penalties. Criminal means criminal prosecution of individuals as well as substantial fines. Successful criminal convictions generally lead to civil lawsuits. Civil lawsuits (especially in class-action situations) can carry substantial financial penalties and damage a company's reputation with its customers.

The Business Impact of Regulatory Compliance

- ☒ **Health Insurance Portability and Accountability Act (HIPAA).** The market to ensure compliance with HIPAA requires that all patient healthcare information be protected to ensure privacy and confidentiality when electronically stored, maintained, or transmitted. HIPAA carries penalties of up to \$250,000 in fines and jail time of up to 10 years.
- ☒ **Gramm-Leach Bliley Act (GLBA).** GLBA mandates privacy and protection of customer records maintained by financial institutions. Noncompliance could subject the financial institution, its officers, and directors of that financial institution to severe penalties, which may include a civil penalty of not more than \$100,000 for each violation.
- ☒ **Sarbanes-Oxley Act.** In the wake of recent financial scandals, the Sarbanes-Oxley Act of 2002 requires public companies to validate the accuracy and integrity of their financial management. Penalties for violation may include fines, imprisonment for up to 20 years, or both.
- ☒ **SEC 17A-4.** SEC 17A-4 is a regulation established by the SEC to establish retention policies for brokers, dealers, and Exchange members. Per SEC 17A-4, broker/dealers are required to archive the electronic communications of licensed professionals for at least three years. The SEC recently announced joint actions against five broker-dealers for violations of record-keeping requirements concerning email communications. The firms consented to the imposition of fines totaling \$8.25 million (\$1.65 million per firm).
- ☒ **USA Patriot Act.** The Patriot Act requires all broker/dealers to know and understand what transactions are taking place within client accounts and requires

them to track and report all suspicious transactions. Failure to comply has costly civil and criminal penalties, including fines up to \$1 million per transaction.

- ☒ **FDA 21 CFR Part 11.** FDA 21 CFR Part 11 is a rule enforced by the U.S. Food and Drug Administration in August 1997 to regulate the use of electronic records and electronic signatures. Manufacturers and authorized distributors that violate the law can incur substantial penalties and civil liabilities, ranging from \$50,000 to \$1 million in civil fines levied against the sales rep or manufacturers/distributors to a felony conviction of up to 10 years in prison. There is also a \$100,000 fine for failure to report a violation.

- ☒ **Basel II.** The New Basel Capital Accord, more commonly known as Basel II, is focused on improving risk and asset management to avoid financial disasters. Part of this compliance dictates that data capture, including electronic messaging, must be fully operational by 2004, and financial institutions must have three years of data on file by 2007.

- ☒ **European Union Data Protection Directive.** The European Union Data Protection Directive specifies that "personal data" must have "appropriate security." The directive sets standards for protecting personal data within the European Union, and it applies to any organization that processes personal data, in both public and private sectors (except law enforcement and other entities regulated by national laws). It also applies to foreign entities that process personal data within the EU.

FIGURE 2

Government and Industry Regulations Impact Matrix

Regulation	Financial Services	Insurance	Banking	Healthcare	Pharmaceutical	Government
Sarbanes-Oxley Act of 2002	Major Impact	Major Impact	Major Impact	Major Impact	Major Impact	Minor Impact
Health Insurance Portability & Accountability Act (HIPAA)	Minor Impact	Major Impact	Minor Impact	Major Impact	Medium Impact	Minor Impact
SEC 17A-4	Major Impact	Minor Impact	Medium Impact	Minor Impact	Minor Impact	Minor Impact
FDA 21 CFR Part 11	Minor Impact	Minor Impact	Minor Impact	Minor Impact	Major Impact	Medium Impact
New Basel Capital Accord (Basel II)	Medium Impact	Minor Impact	Medium Impact	Minor Impact	Minor Impact	Minor Impact
California SB 1386	Medium Impact	Medium Impact	Medium Impact	Medium Impact	Medium Impact	Medium Impact
USA Patriot Act	Major Impact	Major Impact	Major Impact	Minor Impact	Minor Impact	Minor Impact
Gramm-Leach Bliley Act	Major Impact	Minor Impact	Medium Impact	Minor Impact	Minor Impact	Minor Impact
Government Paperwork Elimination Act	Minor Impact	Minor Impact	Minor Impact	Minor Impact	Minor Impact	Major Impact
Electronic Signatures in Global and National Commerce Act (E-Signature Act of 2000)	Medium Impact	Medium Impact	Medium Impact	Medium Impact	Medium Impact	Medium Impact
Check 21 legislation	Major Impact	Medium Impact	Major Impact	Medium Impact	Medium Impact	Minor Impact
Basel II	Major Impact	Minor Impact	Minor Impact	Minor Impact	Minor Impact	Minor Impact
European Union Data Protection Directive	Medium Impact	Medium Impact	Medium Impact	Medium Impact	Medium Impact	Minor Impact

Minor Impact
 Medium Impact
 Major Impact

Source: IDC, 2004

Threat Environment

Email pipelines have become a favorite target for malicious attacks, including worms, viruses, hackers, blended threats, and the like. Viruses remain constant, but worms and malicious code are now the more significant threat to organizations. With a constant stream of new threats, antivirus companies are producing and distributing signature files faster than ever. However, the speed with which new worms and malicious code are spreading has caused the effectiveness of traditional signature-based antivirus solutions to suffer. Recent malicious code incidents have achieved widespread propagation at rates significantly faster than many previous viruses. Worm propagation times have dropped from hours to minutes.

Email pipelines have become a favorite target for malicious attacks, including worms, viruses, hackers, blended threats, and the like.

Moreover, the motive and intention of virus writers has changed. In the past, amateurs seeking notoriety typically created worms and viruses to destroy data. Today, more sophisticated attackers, often organized crime, are increasingly using worms and viruses to obtain credit card numbers, bank account information, and other personal information to perpetrate identity theft. The sophistication and scale of online frauds and identity thefts are increasing at a rapid pace. The recent incidents of "phishing attacks" on banks and their online customers have opened both consumer

and corporate eyes to the increasing dangers of corporate identity theft. Phishing is clearly motivated by financial fraud and gain, and thus criminals are most often behind these attacks rather than teenagers trying to cause havoc.

In the past, spammers traditionally sent spam from their own ISP account. When corporate IT departments and antispam solutions first started to block messages from certain domains and ISP accounts, spammers turned to new methods to conceal their identity. We believe spammers are starting to resort to outright criminality in their efforts to conceal the sources of their spam messages, using Trojan horses to turn the computers of innocent consumers and corporate users into secret spam engines. The explosive growth of cable modems and broadband connections have left consumers and remote employees open to attack. In many cases, their computers are being used as a relay for sending spam to thousands of other people. There is also very little chance that the PC's owner will have any idea their system is being used by a third party.

The Business Impact of Viruses, Worms, and Malicious Code

Our findings show that time spent due to damage caused by viruses coming in via spam is the biggest cost impact felt by organizations, as shown in Figure 3. IDC believes worms and viruses are increasingly using spam techniques — not just the exploitation of unprotected mail relays to maximize spread, but also the use of social engineering to trick victims into opening malicious files.

Time spent due to damage caused by viruses coming in via spam is the biggest cost impact felt by organizations.

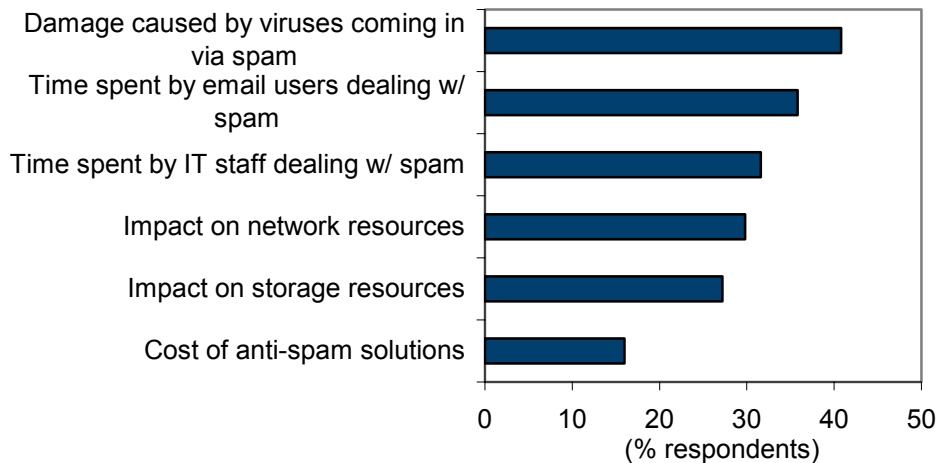
☒ An executive at a major utilities company pointed out to IDC: "Because we're pretty much a Microsoft shop, we're super vulnerable to these spam coming in preloaded with a virus. The problem is they're finding their way in different ways. For example, Web mail, even if we block spam at our SMTP gateway, a lot of people are reading their emails via Web mail with their ISPs, and they're [viruses] getting in that way. Contractors bring their PCs in; users use their PCs at home for their personal ISPs, get infected, come in and that kind of thing. So, it's very huge. With the Nachi worm, just in our department alone, we expended 1,700 hours at \$120/hour cleaning, patching, and stuff like that."

IDC believes this type of story is very common. Moreover, in some cases, senders of unsolicited commercial email (spammers) are also resorting to outright criminality in their efforts to conceal the sources of their ill-sent missives, using Trojan horses to turn the computers of innocent consumers and corporate employees into secret spam zombies.

FIGURE 3

Factors Impacting the Cost of Spam

Q: On a scale of 1 to 5, please rate the cost impact the following have had on your organization
Top 2 responses represented: high [4] and very high[5]



Source: IDC's Spam Study, 2003 (IT Results)

MANAGING THE CHALLENGE

Clearswift: The MIMESweeper Company

Clearswift, the MIMESweeper company, is present in 15 countries worldwide with headquarters both in the United States and in the United Kingdom, and sales offices in Germany, Sweden, Japan, and Australia. Clearswift offers the following messaging security solutions:

- ☒ MIMESweeper for SMTP is an external email solution that protects organizations against inbound and outbound email threats from spam and viruses to employee time-wasting, circulation of pornography, breaches in confidentiality, legal liability, and IT resource misuse.
- ☒ MIMESweeper for Web brings policy-based content security to the HTTP gateway. MIMESweeper for Web analyzes Web content and blocks pages or files that are prohibited by an organizations security policy.
- ☒ SECRETsweeper is a full encryption/decryption and digital signature gateway. In combination with MIMESweeper for SMTP, SECRETsweeper provides gateway signing, encryption/decryption, and policy-based management of the threats associated with encrypted email.

Clearswift secures content and protects against digital attacks by enforcing security policies that increase productivity, reduce IT costs, and create a safer business environment. Its goal is to provide total content security for email and Web. Clearswift enables organizations to protect themselves against digital attacks, meet legal and

regulatory requirements, implement productivity-saving policies, and manage intellectual property passing through their networks.

To address the gaps that exist in the current layered security infrastructure, Clearswift recently announced enhancements to its current product line and the addition of a new policy-based archiving solution. With the addition of the new archiving product, Clearswift meets the overwhelming demands of the market to address regulatory and legal issues brought on by regulatory statutes and compliance laws worldwide. Underpinning the strategic roadmap, Clearswift will provide content security solutions to the market on a range of platforms—software, managed services and appliances. Clearswift's road map is focused on helping organizations address the future of the rapidly changing Internet and email content security market.

CLEARSWIFT CUSTOMER CASE STUDIES

Company: Brother International

Location: Bridgewater, New Jersey

Country: United States

Industry: Manufacturing

Users: 1,100

Respondent: Senior network administrator

Company Profile

Brother International Corporation is one of the premier providers of products for the home, home office, and office. With its corporate headquarters located in Bridgewater, New Jersey, Brother was established in the United States on April 21, 1954 and markets many industrial products, home appliances, and business products manufactured by its parent company, Brother Industries Ltd., of Nagoya, Japan. These products include an award-winning line of multifunction centers and printers. Brother also provides the number 1 line of facsimile machines in the United States and is the leader in electronic labeling, with its full line of P-Touch electronic labeling systems. With revenue of over \$1 billion in fiscal year 2000, Brother and its subsidiaries employ over 1,100 people in the Americas.

Business Challenge

Like most large manufacturers, Brother International operations are worldwide. The benefits of a global organization come with a cost: namely, a complex messaging environment with multiple mail programs, servers, and supported clients. The network administrator we spoke with was not just responsible for all network security at his location, but also connectivity with spoke sites around the globe. Spam was not an issue when the company first implemented a messaging security solution, but that changed very quickly. According to the network administrator, "Spam was not a problem when we first implemented the solution, our main issue was email viruses.

Gradually over the past few years we've gone from about 15,000 emails per day to over 135,000 emails per day. Our reports indicate that over 85% of all inbound traffic is currently junk email."

The network administrator made it clear the problem soon rose to the upper ranks at Brother. "As the amount of spam continued to increase, we started to hear from the CEO and president level. It was also brought up at the board level, and we were tasked with solving the problem immediately. People from C-level executives to order-entry personal were complaining that it took too much time to delete 300 messages. On top of that, our email servers simply could not function with the amount of mail we are getting now."

The Solution: Clearswift

Brother International has been a Clearswift customer for over five years. As mentioned, the solution was first installed before spam was a problem. When spam started to become a problem, the network administrator felt confident Clearswift would address the problem. "We didn't see a need to look at any other antispam solutions. We were very pleased with ability of the Clearswift solution to block email viruses. We view spam as part of a larger messaging security solution, and we expected Clearswift to solve the problem, and they more than met our expectations."

Keeping Things In-House

Brother, like many large organizations, made it very clear they wanted an in-house solution. "We didn't want to outsource for two reasons: First, we had a concern with a third-party having access to our electronic communications. Second, we didn't like the monthly cost per seat of an outsourced solution."

The network administrator went on to tell IDC that, in addition to keeping things in-house, having a flexible and customizable solution was a must. "We tested some appliance-based solutions, but I didn't have the ability to customize to fit our environment. It would take me months to configure a piece of hardware to do what Clearswift is doing now. The Clearswift solution runs itself after initial configuration."

Overall Experience

Brother International made a point to express the quality of Clearswift's customer service representatives. "No one can compare to Clearswift customer service. Their technicians are phenomenal. The annual support contract pays for itself the first time you use it." When IDC asked the network administrator if he viewed spam as a security threat, he summed up his satisfaction by saying "not anymore".

Company: State of Massachusetts

Location: Boston, Massachusetts

Country: United States

Industry: Government

Users: 40,000

Respondent: IT manager for Gateway Security

Company Profile

The State of Massachusetts employs over 40,000 individuals and includes more than 100 individual government agencies, all with different needs and priorities. The Department of Corrections, the Department of Education, the Department of Public Health, the Department of Revenue, the Department of Motor Vehicles, and the Department of State Police are a few examples of the various government departments inside the state.

Business Challenge

The corporate sector is not alone in the fight against unwanted junk mail clogging networks and negatively impacting worker productivity. The government sector has also felt the sting of spam on worker productivity and network resources. The State of Massachusetts told IDC a familiar tale of trying to solve the problem on its own at first. The state first implemented a filter based on key words but quickly found out that managing a home-grown solution was not only time consuming, it also had a high degree of false positives. An IT manager for the State of Massachusetts' Information Technology Division told IDC: "At first, we started off with a small list of key words to handle the spam problem. We found we were spending way too much time on configuration in order to meet the needs of each agency. We also discovered that too many legitimate messages were getting caught in our quarantine because of a key word." The IT manager made it clear to IDC that he needed a flexible solution that could be configured for the needs of each agency in the state.

The Solution: Clearswift

Customization Is Key

The State of Massachusetts implemented the Clearswift solution in 1999 to address both spam and virus infection. After testing many other solutions, they chose Clearswift based on a combination of effectiveness and ease of use. The IT manager told IDC that "We looked at some other commercial solutions but they were too difficult to configure in our environment. We have many different agencies (health, motor vehicles, education, etc.) and what one agency considers spam, another may not. Clearswift provided an easy-to-use management console that lets us create individual policies for each agency."

Effectiveness and Accuracy

The State of Massachusetts did not want to trade-off a higher effectiveness rate in exchange for more accuracy. *Effectiveness* is the ability of the solution to catch spam, and *accuracy* refers to the false positive rate or percentage of legitimate email messages that are incorrectly identified as spam. The IT manager told IDC: "Every piece of email that comes to our 40,000 state workers goes through Clearswift solution. When we first implemented the Clearswift solution, it was immediately effective in catching about 90% of spam entering our networks. I basically just had to tweak the solution for a few of the state agencies, and we were able to catch the remaining 8–10%. You can use it right out of the box but we wanted to make sure we were utilizing the full value of the Clearswift solution. We have been very pleased."

Outbound Email Protection

The State of Massachusetts also told IDC about another important benefit of the Clearswift solution — the need to filter outbound email for inappropriate content. "Again, we looked at some other solutions but they could only address inbound email. Outbound email is very important to us. We look at email just like sending something out on state letterhead. We can not have curse words, chain letters, viruses, and pornographic images being sent out. We stress that our email is a reflection of the Commonwealth of Massachusetts."

CONCLUSION

The IT respondents overwhelmingly indicated that they expect the spam problem to worsen. Almost 76% of IT respondents indicated they expect the spam problem to get worse. In our in-depth interviews with IT executives, two key points were made very clear: first, they expect the volume of spam to continue to increase; second, they believe government legislation will have little to no effect on the spam problem.

IDC believes a multilayered approach to the messaging security infrastructure is necessary to thwart the threats outlined in this document. IDC believes antispam will continue to converge with email content security over the next year. Our results show that two out of three executives view antispam as part of a larger network security solution. We believe some customers will continue to buy point solutions, but this will be the exception, not the rule. Antispam will continue to be an important adoption driver in the messaging security implementation; however, IDC believes it will become a feature of messaging security and not a distinct market.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2004 IDC. Reproduction without written permission is completely forbidden.