The Economics of Spam

Spam. Unsolicited bulk email (UBE). Junk email. Unsolicited commercial email (UCE). Call it what you will, it's become a major headache for companies. The volume of spam emails sent has increased exponentially during recent years, and so has the cost of dealing with that spam. While awareness of the problem has certainly increased, many companies still do not realize the significant impact which spam is having on their profits. Similarly, many do not realize that not all antispam solutions are created equal and that choosing the wrong solution can significantly diminish return on investment. This paper will examine the ways in which spam can impact profits and outline the criteria that every company should consider when choosing its antispam solution.

33 North Garden Avenue
Suite 1200
Clearwater, Florida, USA 33755
Tel: 1-727-562-0101
Tel: 888-688-8457 (US/Canada)

www.sunbeltsoftware.com

Introduction

In 2001, the European Commission reported that spam cost businesses $14 billion worldwide. During subsequent years, the cost has risen considerably. Ferris Research estimates that spam will cost businesses $35 billion in 2007. And that's only in the US. Globally, the cost will be approximately $100 billion, according to Ferris.

Why is spam costing businesses so much more than in previous years? Because there's so much more spam, that's why. Today, more than 50 billion emails are sent each and every day – and more than 50% of those emails are spam. Email systems are, quite simply, being inundated with a completely unprecedented volume of spam. And so are the users of those email systems.

The situation will probably not improve any time soon. For years, spam has been on the rise and it's a trend that looks set to continue. The introduction of antispam legislation in various jurisdictions has not resulted in a reduction in spam, nor have the various antispam coalitions formed by companies such as Microsoft, AOL and Yahoo!. The spammers simply keep on spamming - and they're pushing it out in ever increasing quantities.

Unfortunately, this means that businesses shall have to keep on dealing with spam – and keep on bearing the associated costs.

How spam costs your business money

To delete a spam only takes a couple of seconds, so it cannot be too much of a problem, right? No, wrong. The cost of spam is frequently underestimated in this manner. While the impact of a handful of spams may well be negligible, the impact of tens or hundreds of thousands of spams will invariably be considerable.

To quantify the exact cost of spam is impossible. Some costs will depend on what, if any, antispam solution has been deployed, some will depend on the business environment and others simply cannot be quantified. There is, however, absolutely no doubt that spam costs each and every internet-connected business money.

Some of the costs associated with spam are obvious and fairly well-known. Many people will have seen documents that explain how, if it takes a user X number of seconds to delete a spam and if that user receives Y numbers of spams a day, he'll spend Z number of hours during the course of a year dealing with spam. Similarly, many people will have encountered material that explains spam's impact on bandwidth and storage costs. Both sets of costs are very real – spam can indeed have a significant impact on both staff productivity and the infrastructure. But there are also other, far less obvious costs too and, in order to be able to select an effective antispam solution that will deliver the maximum return on investment (ROI), a business must understand how these costs arise and how they can be minimized. These other costs are not directly attributable to spam, per se; instead, they are the result of the misidentification of email by antispam solutions.

The cost of misidentification

False positives: non-spam emails that are incorrectly identified as spam and blocked. False negatives: spam emails that are incorrectly identified as non-spam and not blocked. Unfortunately, both are inherent in antispam technology and both can dramatically decrease the ROI which an antispam solution was expected to deliver.

Each and every spam email that slips through the net must be manually dealt with by the recipient at a cost to his or her productivity. Additionally, such emails may result in staff being exposed to explicit and

offensive material – and that's something for which the employer could be held legally responsible (see, "Employees could sue over porn spam" in References).

Many antispam solutions provide administrators with the ability to adjust the sensitivity of the spam filter. Upping the sensitivity of the filter will usually decrease the incidence of false negatives – but, unfortunately, will almost certainly increase the number of false positives – and false positives can be extremely costly.

Recently, a Colorado-based law company did not appear at a hearing and was ordered to pay opposing counsel's costs. The law company had upped the sensitivity on its Barracuda Spam Firewall 200 in order to block spam that was still reaching end-user desktops. This resulted in not only the spam being blocked, but also emails from the United States District Court for the District of Colorado, including a notification of the date of the hearing. The law company was left facing a bill of several thousand dollars.

How much "missed opportunities" cost businesses is impossible to quantify. Should an order from a customer be incorrectly discarded as spam it's not only that order which may be lost, but also subsequent orders from that customer. Who wants to deal with a company that appears not to respond to its email?

False positives impact productivity too. A high rate of false positives will result in staff having to expend time carefully checking their deleted or quarantined items to look for misidentified emails. The recovery of such emails can also be a time consuming exercise – especially as some antispam solutions require staff to review quarantined items using a cumbersome web-based system. And time is, of course, money. According to Ferris Research, it costs $3.50 to recover an erroneously deleted email. That may seem like an insignificant amount, but in a company with 1,000 staff, a single misidentified email per month per member of staff equates to an annual cost of $42,000.

To filter, or not to filter: that is the question

Is filtering spam really worthwhile? Do its disadvantages outweigh its advantages? Many companies have asked those very same questions and reached the conclusion that it isn't: they would rather endure spam than risk losing business. But that standpoint makes very little business sense: dealing with misidentifications might be costly, but it's much less costly than dealing with spam manually – in fact, it's about a third less costly.

To filter, or not to filter: that is not the right question. The question that companies should ask is: how to filter and to filter accurately?

The real test of a spam filter is not how much spam it can stop, but how much spam it can stop without also stopping other email. Misidentifications cannot be completely eliminated – as mentioned previously, even the best antispam solution will misidentify some emails and any vendor that claims otherwise is simply not being honest. That said, not all solutions are created equal and some are far more accurate than others. By choosing a solution which minimizes the incidence of misidentification, a company can both protect its staff and maximize its ROI.

How to ensure that a spam filter will deliver the maximum ROI

There are numerous antispam solutions on the market, but how should a company choose between them? There are 6 essential criteria which should be considered and these are discussed below.

- **Does the solution have auto-whitelisting capabilities?**
    A whitelist is a data file of addresses and/or domains which is used to instruct the spam filter to ignore email from those addresses or domains. Many antispam solutions support whitelisting and it's an effective method of reducing false positives – but traditional whitelisting mechanisms are neither perfect nor easily implemented. Creating a comprehensive whitelist can be both difficult and time consuming. To make the process easier, some solutions enable address books to be imported into the whitelist. This certainly makes creating a whitelist a speedier process, but it provides no assurances that post-import additions to address books will be whitelisted – or that contacts who were never added to the

address book to begin with (a surprising number of people do not add all their contacts to their address book and instead rely on their email client's auto-complete).

To address such shortcomings, a number of antispam solutions now enable companies to optionally select to automatically add recipients of outgoing messages to their whitelist. This self-learning capability makes whitelist management much easier and also eliminates the possibility of human error resulting in addresses not being whitelisted.

Auto-whitelisting can drastically cut the number of potentially costly and damaging false positives and help the solution deliver the maximum possible ROI.

- **Is the solution server-based or a hardware appliance?**

    Desktop-based solutions are considerably more expensive than either server-based solutions or hardware appliances. Why? Primarily because it costs far more to install and maintain a solution on each networked desktop than to install and maintain a solution on the server or to install an appliance. The licensing costs for desktop-based solutions tend to be greater too. Additionally, unlike server-based products and appliances, desktop solutions do not prevent spam from entering the physical infrastructure: spam will still consume both bandwidth and storage capacity.

    For an antispam solution to be cost effective, it must either be server-based or an appliance; desktop-based products are simply a false economy.

- **Does the solution provide multiple detection mechanisms?**

    Spammers need their email to reach people and so are constantly seeking out new ways of getting their messages past spam filters and onto desktops – and their methods are becoming increasingly varied and sophisticated. To avoid RBL blocking, spam is sent from home computers that have been co-opted into botnets. To conceal content from spam filters, characters and words are hidden inside the layers of a GIF and further obfuscated by blurring or speckling. Word salads are used to confuse Bayesian filters. And these and other methods are often used in conjunction.

    Such diversity means that no single detection mechanism is able to stop all spam. To provide the maximum protection, an antispam solution must leverage a combination of multiple detection mechanisms including heuristics, RBL checking (DNSBL and SURBL), blacklisting and whitelisting, Sender Policy Framework (SPF) validation and must have the ability to inspect attachments and embedded objects.

- **Does the solution enable the easy review of suspected spam?**

    Email will occasionally be misidentified – as already mentioned, it's inevitable – and that means that end users will need to check quarantined messages. Some antispam solutions do not make this easy to do: users need to logon to a web-based system and review and delete such messages one-by-one. This can be a time consuming process that impacts productivity. It may also act as a deterrent to users checking their quarantined items – and that could lead to important emails being missed.

    To enable users to review in the shortest possible time and most efficient manner, an antispam solution must mark and redirect suspected spam to users' inboxes.

- **Does the solution offer complete protection for the messaging infrastructure?**

    Messaging infrastructures must be hardened against a variety of threats. Phishing scams, viruses, adware and spyware can all effect productivity, result in expensive downtime or the exposure of sensitive company information. Deploying a different solution to protect each threat adds to the complexity of the infrastructure and makes management a more difficult and time consuming process.
    To provide the infrastructure with maximum protection and to enable efficient and streamlined management, an antispam solution must do more than simply protect against

spam: it must also integrate protection against phishing scams, viruses and other forms of malware.

How Sunbelt Software's VIPRE Email Security for Exchange solution combats spam and other threats

Sunbelt Software's VIPRE® Email Security for Exchange (formerly Ninja Email Security) provides complete protection for the messaging infrastructure.

VIPRE Email Security for Exchange
VIPRE for Exchange is an add-on for Microsoft Exchange Server 2000, 2003 and 2007. With an expandable plug-in based architecture, VIPRE for Exchange provides future-proofed security for Exchange environments and its features include:

- **Multiple spam detection mechanisms**
  VIPRE for Exchange combines Cloudmark's antispam engine with Sunbelt's own image-spam and antispam engines to provide companies with an unparalleled level of protection against spam. To ensure that almost all spam is blocked while minimizing misidentification, VIPRE for Exchange leverages multiple detection mechanisms including heuristics, DNSBL and SURBL checks and SPF validation and more.

- **Automatic whitelisting**
  To substantially reduce the possibility of misidentification, VIPRE for Exchange automatically whitelists the recipients of outgoing emails.

- **Complete protection for the messaging infrastructure**
  To provide maximum protection for the infrastructure, VIPRE for Exchange leverages multiple industrial strength antivirus engines, including Sunbelt's own VIPRE antivirus engine. and provides integrated protection from phishing scams, spyware and other forms of malware.

- **Streamlined administration**
  VIPRE for Exchange was designed by admins for admins to make both deployment and management easy. According to a study by Osterman Research, VIPRE for Exchange takes 50% less time to deploy and 50% less time to manage than competing products (see References). No matter what size a company may be, this can result in substantial savings and help maximize ROI.

- **Easy review of suspected spam**
  To enable users to easily and speedily review suspected spam, VIPRE for Exchange can be configured to mark emails with a customizable Subject-line identification and to redirect to a quarantine folder in users' Exchange mailboxes.

- **Global and policy-based disclaimers**
  Add a disclaimer to all email or to allow users to bypass the global disclaimer on a per email basis or to add different disclaimers for different groups of users. VIPRE's global and policy-based disclaimers provide the ultimate in flexibility and configurability.

VIPRE Email Security for Exchange provides robust and comprehensive protection against spam, viruses, phishing, zero-day attacks and more. Many organizations are choosing to protect their corporate email by implementing layered protection at the server and perimeter.

Sunbelt recognizes that email systems are mission-critical and must be available 24/7/365 and offer options for 24/7/365 technical support by telephone, email and web forum.

To find out more about VIPRE for Exchange please visit: www.sunbeltsoftware.com.

About Sunbelt Software

Headquartered in Tampa Bay (Clearwater), Florida, Sunbelt Software was founded in 1994 and is a leading provider of Windows security software including enterprise antivirus, antispyware, email security and malware analysis tools. Leading products include the VIPRE® and Counterspy® product lines, VIPRE Email Security for Exchange, Sunbelt Exchange Archiver™, CWSandbox™, and Threat Track™.

For more information about Sunbelt Software, please visit the company's website at www.sunbeltsoftware.com.   To learn more about current activities, products and ideas at Sunbelt Software, please visit Sunbelt's corporate blog at www.sunbeltblog.com.

References

Junk e-mail costs internet users €10 billion a year worldwide - Commission study
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/01/154&format=HTML&aged=0&language=EN&guiLanguage=en

Industry statistics – Ferris Research
http://www.ferris.com/research-library/industry-statistics/

America Online, Microsoft and Yahoo! Join Forces Against Spam
http://www.microsoft.com/presspass/press/2003/apr03/04-28JoinForcesAntispamPR.mspx

Employees could sue over porn spam
http://news.zdnet.co.uk/security/0,1000000189,39153163,00.htm

Spam filter costs lawyers their day in court
http://www.washingtonpost.com/wp-dyn/content/article/2007/07/13/AR2007071300606.html

Pace v. United Services Automobile Association, Case No. 05-cv-01562-LTB-MJW, D. Co., 2007 U.S. Dist. LEXIS 49425, July 9, 2007
http://spamnotes.com/files/31236-29497/Pace.pdf

Spam Cost Report 2005 (Ferris Research)
http://www.ferris.com/2005/02/24/the-global-economic-impact-of-spam-2005

Blacklist Statistics Center
http://stats.dnsbl.com/

Comparing Email Management Systems that Protect Against Spam, Viruses, Malware and Phishing Attacks (Osterman Research)
http://www.sunbelt-software.com/documents/Sunbelt-Messaging-Ninja-Comparing-Email-Management-Systems-that-Protect-Against-Spam-Viruses-Malware-Phishing-Attacks.pdf