The Good, the Bad and the Ugly

Ridding Your System of Unwanted E-Mail

by Gleb Budman

Businesses today are under attack from a variety of unwanted e-mail. Often spam gets most of the attention from e-mail users and system administrators, and perhaps rightly so. It is estimated that more than 70 percent of e-mail sent in the United States is commercial spam.

However, e-mail threats come in many forms, including more dangerous e-mail in the form of phishing (a form of e-mail fraud), viruses and directory harvest attacks. These security threats aren't static. Change comes quickly, punishing those who are unprepared. While many companies have point solutions for individual threats, new blended attacks can sail right through traditional information technology defenses.

As the types and sophistication of e-mail threats increase, their seriousness also escalate. Unwanted e-mail hampers productivity, increases IT costs and increases corporate liability through security breaches or inappropriate e-mail content reaching employees.

Spam: The Monday Morning Sort

Dealing with spam in the corporate environment has become quite expensive. Employees can spend hours each day weeding through their inbox, and as a result companies are losing days of employee productivity. In 2003, corporations spent more than $20 billion dealing with spam-related issues, according to Ferris Research.

Lyndon Brown, Wyndham International's manager of network services and electronic messaging systems, estimates that the company lost more than 35 hours every business day dealing with spam—more than four full-time employees per year—before the company found a way to eliminate unwanted e-mail. This lost time was in addition to IT dealing with lost e-mails, questions, issues and complaints. "In order to keep up with ever-increasing demands of managing network security, addressing user needs and delivering high-quality customer service, no company can afford to spend more hours than there are in a day just managing spam filtering," said Brown.

The Tidal Wave of E-Mail

High volumes of unwanted e-mail are not only a nuisance and a productivity issue, but they can also overload critical IT infrastructure. For Wyndham the company's growth and success brought e-mail system challenges as inbound e-mail volume approached 100,000 messages per day. That volume will apply significant pressure to any IT infrastructure, but it is especially problematic with the added burden of e-mail threats.

As with many hospitality firms, Wyndham relies on its e-mail systems to maintain a high-profile public presence and provide incomparable customer service. Over time the percentage of inbound spam climbed to unreasonable levels. According to Brown, "Close to 70 percent of Wyndham's incoming e-mail was spam."

This volume of e-mail can be a problem with certain e-mail solutions. In its search for protection, Wyndham found that load management was one critical factor. "As we were approaching the six-figure message mark, we needed a solution that was ready for prime time," said Brown. In addition to being overly complex to manage, Wyndham found that some products on the market simply could not handle their message volume. "The very same appliance we spent so much time preparing to use died after 12 hours in real-time production; the replacement sent by the vendor only lasted eight," said Brown.

Spam's Bigger, Badder Cousin – Phishing

Don't be fooled, phishing is not spam. While spam shouts for attention, phishing e-mails arrive masked in familiarity. Phishing is a type of fraudulent e-mail that appears to come from trusted sources such as company management, the IT team or partners. These fraudulent e-mails can use legitimate company graphics, layout, content and links, and ask employees to take actions that seem reasonable in a business context, such as verifying company information. Companies that keep valuable information, like credit card and personal information, including hotels, can be especially at risk for attack. Really though, all companies are at risk.

According to an April 2004 survey from Gartner, an estimated 57 million Americans think that they have received a phishing e-mail[1], and the problem is growing. In a recent online poll conducted by Issues and Answers Network, Inc., 28 percent of U.S. adults inaccurately identify phishing e-mail scams—proving the difficulty in identifying these malicious and increasingly sophisticated e-mails.

A simple e-mail appearing to come from the internal IT department may instruct an employee to reauthenticate their network login for security updates. By responding, the employee unknowingly gives criminals direct access to corporate systems, leading to security breaches, exposure and theft of proprietary information and the related liability. With systems now compromised IT has no choice but to recall and reissue all secure identification methods, check all devices for malicious software and trace systems for any evidence of unauthorized activity.

"Companies in hospitality need to pay attention to the dangers of phishing directed at employees whether the focus is getting consumer information or attacks at your business systems," said Brown. "Phishing attacks are cause for

alarm, since a simple response can open corporate systems to criminals and wreak havoc with technology and legal problems."

Protecting Your Organization

With unwanted e-mail volume increasing at unbelievable rates, everyone is under pressure to protect both their systems and employees from the nuisance and dangers. What can hoteliers do to protect their employees and their systems from the dangers of unwanted e-mail? Many companies have implemented "good enough" solutions to address a piece of the problem, such as virus protection, or are using one tool to address multiple threats, but traditional point solutions can no longer effectively protect organizations against the rapid evolution of e-mail security threats.

Think effective, easy and staying a step ahead when selecting an e-mail security solution. Some of the considerations include:

Effectiveness

Stop unwanted e-mail before it reaches internal systems. A solution that leverages multiple analysis methods to accurately assess whether an e-mail is good or unwanted e-mail can effectively prevent security problems. Performing this analysis before e-mail reaches the inbox also improves system performance by reducing load and enhances IT productivity.

Utilize user-level customization. Different e-mail demands of internal departments require an e-mail security solution that recognizes the unique messaging behavior of each business user and automatically adapts filtering appropriately. While your frontline hotel reception and finance teams need tight e-mail restrictions, customer service or marketing may need to customize their settings to allow competitor promotional e-mails through.

Ease of Use

Ensure simple deployment. An e-mail security application should work effectively with existing support infrastructure and processes to minimize installation time and save the IT team from hours of work.

Minimize IT administration for the system. A comprehensive e-mail security solution should eliminate the need for user e-mail management without shifting the burden to IT. An e-mail security application should self-tune and self-manage. Depending on the system complexity, the administrator should spend just a few minutes a week on day-to-day management.

Staying a Step Ahead

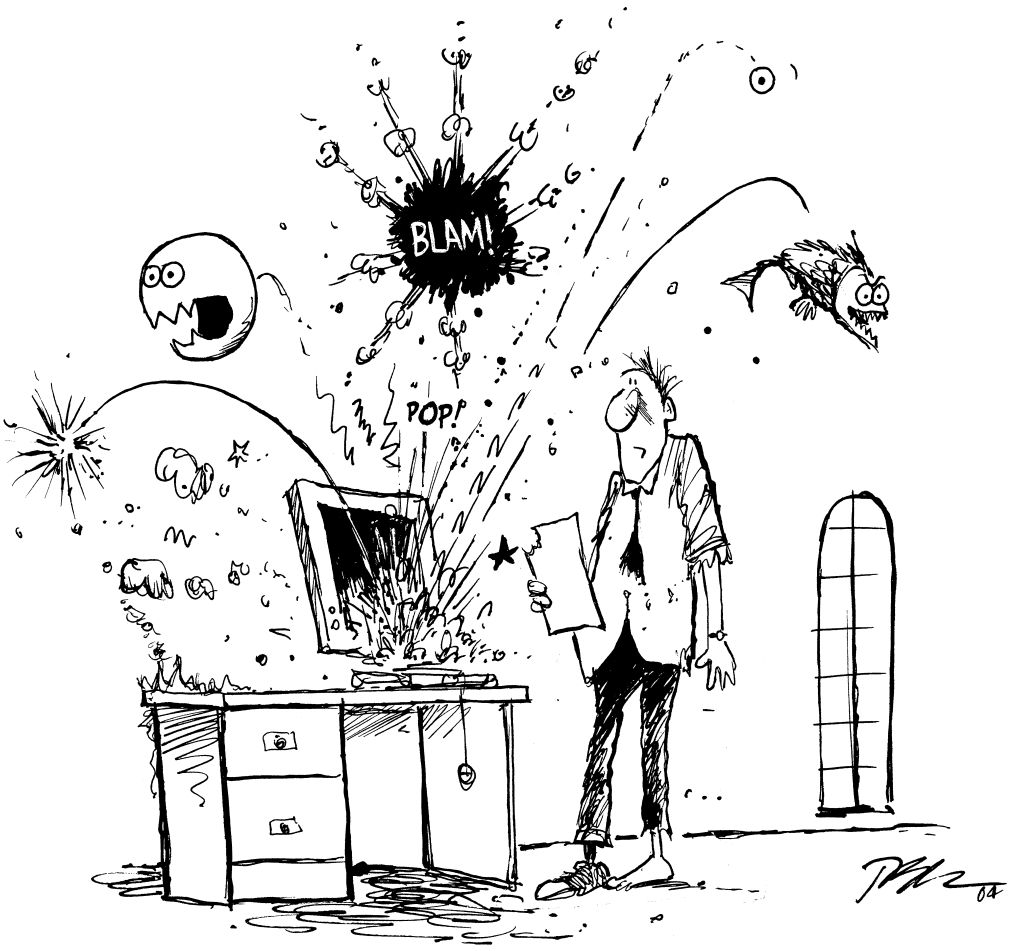
Adapt to new threat developments. Given the rapid evolution of e-mail threats, an adaptive e-mail security solution can provide real-time response. A system that shares information with a larger networked community can provide the fastest and most up-to-date protection against a variety of evolving e-mail threats.

Use a holistic approach. The system should contain not only the threat at hand but also prevent collateral damage to internal systems. If a hotelier experiences a directory harvest attack, does the system recognize and protect against that attack, as well as launch into proactive mode to prepare for a possible phishing or spam attack later using the addresses that were harvested?

Businesses need an integrated game plan to protect themselves against e-mail threats. Take care to understand all your e-mail security needs and select the most effective, easy and advanced application for eliminating unwanted e-mail. With proper protection e-mail can continue to serve as your most effective business communications tool.

Gleb Budman is senior director of product management for MailFrontier, an e-mail security company that protects against spam, viruses, phishing, fraud and the growing number of other costly e-mail threats.

[1] Gartner FirstTake "Phishing Attack Victims Likely Targets for Identity Theft," Litan, Avivah, 4 May 2004.



"...Someone call IT. The spam's getting out of hand again...."