Aberdeen Group
A Harte-Hanks Company

Send to a Friend

The Ins and Outs of Email Vulnerability

July 2007

Aberdeen Group
A Harte-Hanks Company

Executive Summary

As email is business-critical, every organization needs to understand how email is making them vulnerable. Without concrete action, they risk lost productivity, lost data, lost business and punitive damages. This report focuses on the threats posed by both inbound and outbound email as well as the strategies, capabilities and technologies Best-in-Class companies use to mitigate these threats.

"Some things need to be a matter of course. It's not difficult to have all your email encrypted. Why isn't everybody doing it?"

IT Manager – Leading Global Bank

Best-in-Class Performance

Aberdeen used three key performance criteria to distinguish Best-in-Class companies:

- 97% report a decrease in lost productivity as the result of email attacks
- 71% report a decrease in the helpdesk time / cost to remediate email infections
- 85% report no or occasional complaints from email users about spam in their inboxes

Competitive Maturity Assessment

Survey results show that the firms enjoying Best-in-Class performance shared several common characteristics:

- 84% of Best-in-Class organizations report decreasing the number of incidents of viruses, Trojans, spyware, botnets or other malware contracted from email
- 71% of the Best-in-Class report a decrease in the number of data loss incidents associated with email
- 65% of the Best-in-Class have decreased negative publicity associated with email-related events
- 63% of the Best-in-Class have decreased the total cost associated with recovery and remediation from email attacks

Required Actions

In addition to the specific recommendations in Chapter Three of this report, to achieve Best-in-Class performance, organizations must:

- Develop comprehensive email security strategies that address both **inbound** and **outbound** vulnerabilities
- Actively monitor, assess and address email vulnerabilities on an ongoing basis – new threats appear daily
- Include email vulnerability assessment in an overall threat analysis, looking at threats across email and the Web as well as across desktops, laptops, servers and networks

Send to a Friend

Aberdeen Group
A Harte-Hanks Company

Table of Contents

Figures

Tables

Aberdeen Group
A Harte-Hanks Company

Chapter One: Benchmarking the Best-in-Class

Understanding the Threat

Organizations that do not actively assess and address the vulnerabilities represented by email face lost productivity, lost data, and the potential of punitive damages as a result of failing to adequately protect sensitive data. Conversely, organizations that have actively pursued effective email security are realizing concrete gains in productivity, decreasing costs and reduced risk.

Bad Stuff Coming In

Both the volume of unwanted email and the sophistication of email threats are at an all-time high. Email industry experts claim that as much as 90% of all email sent is spam. Our survey responders say that somewhere between two thirds and 80% of the mail they receive is spam.

Email spam threats include infecting the recipient's machine with some sort of malware including spyware and key loggers aimed at capturing sensitive data, as well as viruses, worms and Trojans that can destroy the recipient's disk.

Spam can lead to software being installed on the user's machine that turns that machine into a zombie – a machine that, unbeknownst to its owner, has fallen under the control of someone else who, in turn, can use that machine to send out blasts of spam or mount a denial of service attack. Zombie machines are connected together into *botnets* – networks of zombies – easily manipulated from afar. This year the F.B.I. identified more than a million zombie machines – experts believe there are more likely 7 or 8 million, with new victims daily.

The vogue in email attacks is a simple email directing the reader to a malicious site. When the user visits the site, maleficent code is downloaded to the user's machine. Experts are detecting some 5,000 new malicious sites daily.

Phishing attacks – email purporting to be from a trusted source, created to garner credentials from the prey – have gone from blatant to extremely subtle, and from mass-market blasts to personalized attacks focused on individuals. For example, early phishing forays targeted the customers of the biggest brands – big banks like Citibank and Wells Fargo. Newer generations of phishing scams target smaller regional banks and credit unions and are being referred to as "puddle phishing." Still more targeted attacks such as those that identify specific, high profile individuals, like one recently in the news that targeted specific CEOs, have garnered the epithet "spear phishing."

Bad Stuff Going Out

Aberdeen research found that although most organizations are attempting to stop unwanted email from getting in, significantly less focus is being put on the vulnerabilities inherent in sending email out. **93% of responding organizations filter inbound email for spam and viruses, etc., but only 58% ensure that their outbound email is free of malware.**

Fast Facts

- √ **70%** of all organizations experienced some sort of virus, worm or Trojan infection as the result of email within the last 12 months; 5% experienced more than 100 instances.
- √ **44%** of all organizations experienced data loss incidents through email, while 22% don't know or don't measure – meaning that the incidence is likely much higher.

"Security has to be a layered thing" says the CIO of a major metropolitan transportation governance organization, who attributes his organization's success to using multiple solutions that address both the inbound and outbound sides of the issue. "We use hosted, managed email and, as a result, have never lost email, despite major interruptions. We also use solutions on the desktop to ensure that our machines don't get infected any other way."

Machines can get infected from many sources other than email – from malicious web sites or from tainted files delivered through other media, to name two. Once infected, machines can infect others inside the organization as well as those belonging to prospects, customers and business partners. Machines infected with spyware or key loggers can serve up proprietary information. Zombie machines can send out malicious mail from the company domain.

Contaminated outbound mail is only part of the outbound problem. Email carrying sensitive data is responsible for data loss or leakage on several fronts:

- Inadvertent email – email sent accidentally to someone unintended
- Unprotected email – email sent in the clear (unencrypted) is an easy target for would-be snoopers
- Data theft – email used to transmit sensitive data for nefarious purposes.

Maturity Class Framework

Aberdeen used three key performance criteria to distinguish Best-in-Class companies from Industry Average and Laggard organizations.

Table 1: Companies with Top Performance Earn Best-in-Class Status

Definition of Maturity Class	Mean Class Performance
Best-in-Class: **Top 20%** of aggregate performance scorers	• **97%** report decrease in lost productivity as the result of email incidents • **71%** report decreased help desk time / cost to remediate email related infections • **85%** of email users complain about spam only occasionally or never
Industry Average: **Middle 50%** of aggregate performance scorers	• **13%** report decrease in lost productivity as the result of email incidents • **24%** report decreased help desk time / cost to remediate email related infections • **74%** of email users complain about spam only occasionally or never

Definition of Maturity Class	Mean Class Performance
Laggard: **Bottom 30%** of aggregate performance scorers	• **0%** report decrease in lost productivity as the result of email incidents • **0%** report decreased help desk time / cost to remediate email related infections • **0%** of email users complain about spam only occasionally or never (they all complain to some degree – 23% daily, 70% weekly, 7% monthly)

Source: Aberdeen Group, July 2007

Best-in-Class PACE Model

Achieving Best-in-Class results requires a combination of strategic actions, organizational capabilities and enabling technologies that can be summarized as follows:

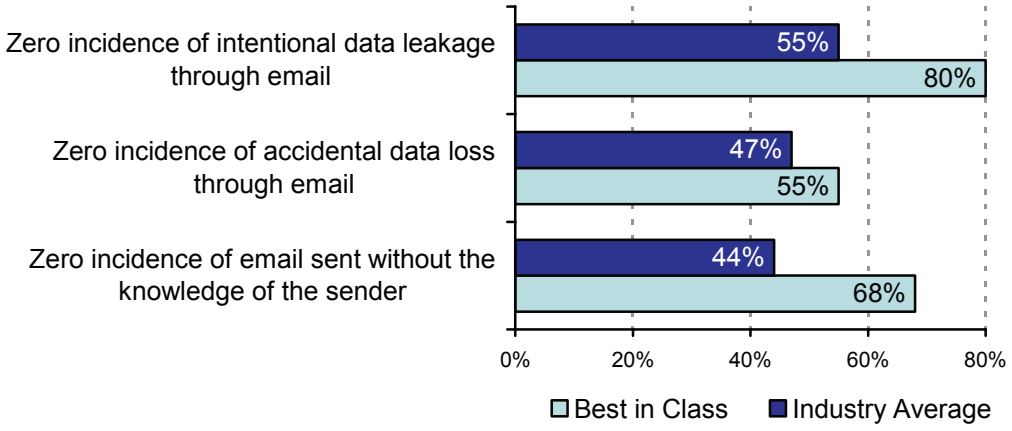
Table 2: Best-in-Class PACE Framework

Pressures	Actions	Capabilities	Enablers
• Reducing productivity loss associated with unwanted email	• Protect users from unwanted email and inbound email vulnerabilities • Prevent the dissemination of spam or infected email from the organization	• Ability to identify and respond to new threats in a timely and automated manner • Email security policy; Role-based email policy • Integration of email security and Web security; Visibility into threats across resources • Protection for email in transmission; scanning of outbound messages	• Email filtering that includes behavior, sender reputation analysis, definable rules, policies and unacceptable terms • Data loss prevention software especially solutions that monitor, alert, and are capable of preventing sensitive data being leaked through email • Email / gateway appliance • Email encryption • Email threat analysis dashboard • Integrated email / web security solution • Monitoring outbound email

Source: Aberdeen Group, July 2007

As shown in Figures 1 and 2, Best-in-Class companies are doing a significantly better job of protecting themselves against outbound threats, including data loss associated with outbound email and email being sent out without the knowledge of email user (by botnets, for example).

Figure 1: Best-in-Class Compared to Industry Average – Outbound Threats

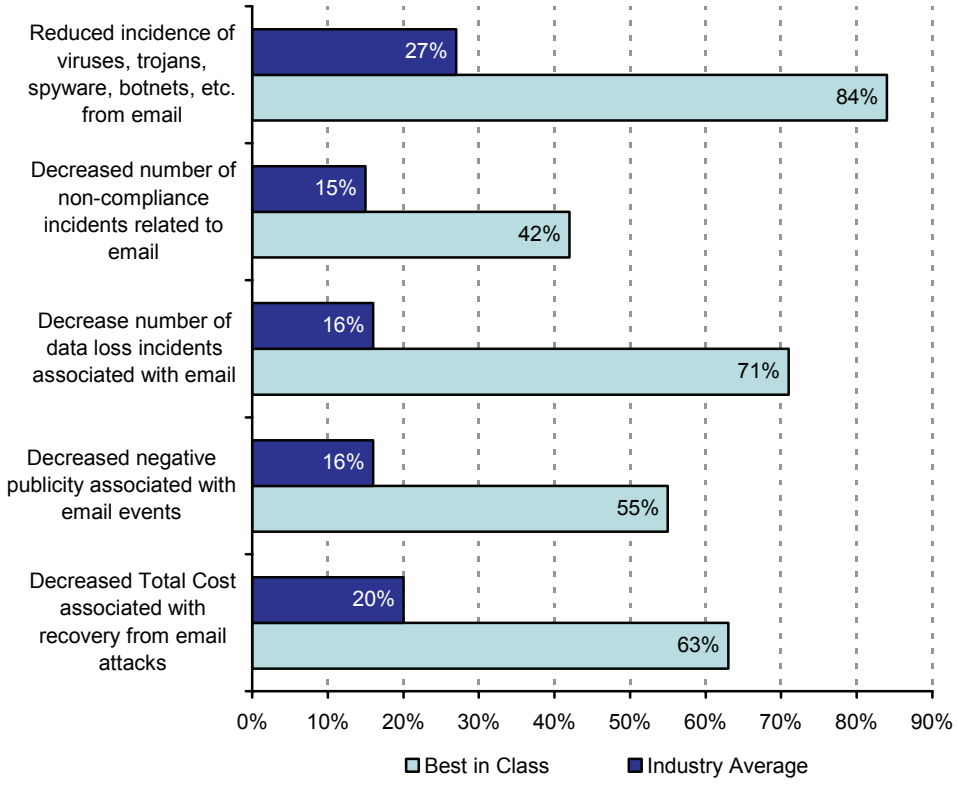


Source: Aberdeen Group, July 2007

Many data loss prevention solutions directly address data loss through outbound email. More Best-in-Class companies have implemented data loss prevention solutions than companies in either the Industry Average or Laggard class, but the Industry Average and Laggard classes are planning to catch up. Sixty-one percent of the Industry Average and 54% of the Laggard companies are **planning to implement** data loss solutions.

Year over year, Best-in-Class companies have done a dramatically better job in reducing the costs and consequences associated with email events. Despite the increased volume and sophistication of attacks, the Best-in-Class companies are making concrete progress.

Figure 2: Best-in-Class compared to Industry Average Performance



Source: Aberdeen Group, July 2007

Email attacks hurt organizations in many ways. Viruses, Trojans, spyware, botnets and all sorts of email-borne malware cripple computers, compromise data security, and turn control over to strangers. Spam and infected email sent out from an organization damages the organization's brand. Losing sensitive data can hurt an organization's trusted brand and make it subject to penalties for failure to secure data protected by regulation. The fact that the Best-in-Class companies are making great strides in reducing the incidence of and the cost associated with the remediation of email exploits shows that progress is indeed possible despite the escalation of threats.

Aberdeen Insights – Strategy

Best-in-Class companies understand the threats that email poses and work to shore it up on all fronts. They protect the email itself in transit, protect their users from incoming threats, and they protect the organization from accidental and intentional data leakage. They create and enforce rule-based email policies and have individuals responsible for evaluating suspicious email and email usage. They actively pay attention to all threats including email. Their approach to email is very intentional and goes well beyond what gets delivered with basic email software.

In the next chapter, we see what the top performers are doing to achieve these gains.

Aberdeen Group
A Harte-Hanks Company

Chapter Two:
Benchmarking Requirements for Success

To cover the gamut of email threats requires a spectrum of technologies not always found in any one solution. For example, most organizations recognize that the spam filtering bundled into their email software is not sufficient to address all the threats that email posesses. Further, unless email threats are taken in a broader context – looking across the organization's resources, for example – the import of a particular threat may be overlooked. For example, when an email message leads the user to a threat on the Web, if nothing is being done to stop the user from going to that malicious site, how will the threat be stopped? Detecting malicious email is one thing – protecting the user from going to a site that's known to be dangerous is another.

Aberdeen research reveals that Best-in-Class companies deploy a variety of technology enablers to better thwart the threats posed by email. As organizations recognize the functionality required to address these threats, they are turning to vendors that can incorporate more and more of the needed functionality into a single offering. Although the Best-in-Class use many technology enablers, they typically use only a handful of vendors – 93% of Best-in-Class organizations use three vendors or fewer.

Fast Facts

- √ 100% of Best-in-Class companies filter inbound email for spam and viruses.
- √ Best-in-Class companies are 63% more likely to employ an email or gateway appliance as part of their email security strategy.

Case Study: Leon County Board of County Commissioners

One Best-in-Class organization, the Leon County Board of County Commissioners, supports more than a thousand users across 36 sites. The Board's CIO, Pat Curtis, says that about 2/3 of the email they receive is spam; but, using two different vendors – one on the desktop and one on the server, the spam doesn't interfere with the some 60,000 legitimate messages they receive daily.

The Board uses email as a collaboration tool and its communications are a matter of public record. As such, they hold over 14 years of email archive. Email for agencies within the county that traffic in sensitive data, such as the courts and agencies handling patient information, is segregated and encrypted.

Curtis says their email is highly reliable and they are very satisfied with their email strategy. Their record proves it. Leon County has:

- Reduced the lost productivity attributable to email
- Reduced help desk time and the cost to remediate email events
- Reduced the number of incidents of viruses and other malware contracted from email, and
- Reports zero incidents of downtime from email and zero data loss events over the last 12 months.

Competitive Assessment

Aberdeen used the aggregated performance of the surveyed companies to determine their ranking: Best-in-Class, Industry Average or Laggard. In addition to having common performance levels, each class also shared characteristics in five key categories: (1) process (the ability to detect and respond to new email threats without placing additional burdens on the organization); (2) organization (the organization's commitment to take responsibility for email use and email security as evidence by such

things as user training and designating responsibility for ongoing email concerns); (3) knowledge management (the gathering and analysis of information critical to understanding and remedying email threats and their consequences); (4) technology (the technologies chosen to address the several aspects of email vulnerability); and (5) performance measurement (the ability of the organization to measure the benefits of technology deployment and use the results to improve key processes further). These characteristics (identified in the table below) serve as a guideline for best practices and correlate directly with Best-in-Class performance across the key metrics.

Table 3: Competitive Framework

	Laggards	Average	Best-in-Class
Process	Timely identification and automated response to new threats		
	49%	52%	71%
Organization	Defined email security policy		
	61%	70%	77%
	Role-based email policy		
	25%	25%	55%
Knowledge	Email threat reports		
	38%	44%	55%
	Visibility into threats across desktops, servers and networks		
	27%	33%	65%
Technology	Robust solutions for inbound email security*		
	41%	49%	65%
	Encryption or Protection for email in transition		
	32%	38%	60%
	Email gateway appliance		
	40%	40%	65%
	Robust outbound email strategy**		
	47%	61%	69%
	Data loss prevention		
	18%	32%	43%
	Track infections from email		
	36%	45%	72%

Source: Aberdeen Group, July 2007

*Various components strengthening inbound email protection – expanded in text below

**Various components strengthening outbound email protection – expanded in text below

Best-in-Class companies are attentive to email threats on every front:

- They automate processes to deal with the fact that new threats appear daily
- People are actively engaged in assessing email abuse and threats
- They have visibility into threats across resources
- They use a spectrum of technologies to protect email
- They're more apt to measure the loss

Organizational Capabilities and Technology Enablers

A coherent strategy to secure email requires addressing the problem from many perspectives. Important in creating the strategy is the understanding that new email threats arise every day, that Internet fraud and data theft are big business, and that a strategy that works is one that acknowledges the dynamic nature of the threat and is designed to identify and respond quickly. Seventy-one percent of the Best-in-Class use technology to identify new threats and automatically respond.

Quote

"About 80% of the email we receive is spam. I personally receive about 2000 legitimate email on a daily basis. Clearly we need a solution that can handle our volume and not all solutions do."

Managing Director, UK-based Technology Company

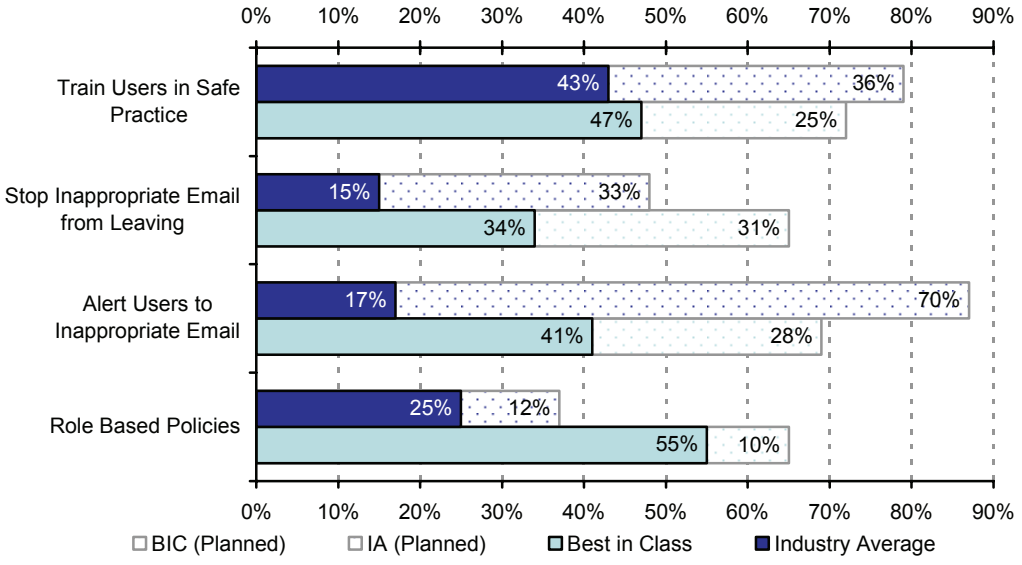
Bolstering Inbound Protection

In addition to the quick detection of new threats and automatic response, Best-in-Class companies are more apt to use anti-spoofing, anti-phishing, anti-spyware, anti-fraud and anti-key-logger solutions than the Industry Average or Laggard Class. They're more apt to verify the email sender's authenticity, and they are more apt to correlate email and Web threats to detect threats that exploit both media.

Bolstering Outbound Protection

On the outbound side, Best-in-Class companies do a better job of ensuring that outbound messages are malware free. They are also more apt to protect email messages in transit. Although the Best-in-Class have deployed more capabilities to protect their email, the Industry Average and Laggard Classes are making plans to catch up, as shown in Figure 3.

Figure 3: Best-in-Class Compared to Industry Average Capabilities



Source: Aberdeen Group, July 2007

When it comes to protecting sensitive data, organizations are best served by creating role-based policies that can be used to ensure that those sending sensitive data are doing so appropriately. Alerting users to inappropriate use and even stopping

inappropriate mail from leaving are among the strategies used to stop data from leaking through email. Making sure that email is protected in transmission is critical. Sending email "in the clear", that is email that is not encrypted, is tantamount to sending the message on a postcard – it's easily read in transit by anyone that knows how. Training users on safe email usage saves users from being duped into divulging sensitive data or their machines from being infected. The Best-in-Class are using and evaluating reports on email usage and threats as well as looking at threats across the organization's resources.

Creating Layers (Tiers) of Protection

Applying the sound security strategy of creating layers or tiers of security to the threats posed by email means that organizations protect themselves against email at various points. Some companies choose to outsource their email management, keeping one level of email security outside the organization itself. Others use an email or gateway appliance to handle email as it enters and leaves the organization's network, stopping bad email from coming into the organization and inappropriate email from leaving the organization.

In most cases organizations also use anti-virus protection on their desktops and laptops – a different layer of protection. Anti-spyware, anti-phishing, anti-malware solutions might be applied at the email server or on desktops and laptops. Data loss prevention solutions might be added to create another layer of protection on the outbound side. Because new threats emerge daily, creating tiers or layers of protection helps organizations defend themselves better because one set of protections might be better against certain attacks, and another set better against others.

Aberdeen Insights – Technology

Because email is used by every organization, and because email users vary widely in technology savvy – email is used by experts and novices alike – it's a good target for broad-based malicious email campaigns that rely on the probability that someone somewhere will open a malicious message or go to a malicious site.

As long as there's profit to be had, the incentive to develop ever-more pernicious threats exists, and it's likely that threats that exploit vulnerabilities in email will continue to grow in volume and sophistication.

Organizations need to take a tiered approach to email security – keeping the threats as far away from the email users as possible, and relying as little as possible on the technology expertise of the email user. Likewise, organizations must assume that their environments are the targets of threats on every channel and prevent infected email from leaving.

In addition, data loss / data leakage events that use email create additional threats. Without some work to define and automate process, organizations have little chance of stopping sensitive data from leaving.

Aberdeen Group
A Harte-Hanks Company

Chapter Three: Required Actions

Whether a company is trying to move its performance in email security from "Laggard" to "Industry Average," or "Industry Average" to "Best-in-Class," or simply to maintain its "Best-in-Class" advantage, the following actions will help them identify their next steps:

Fast Facts

- Best-in-Class companies are more than twice as likely as the Industry Average and Laggard classes to alert users to the sending of inappropriate email
- Best-in-Class companies are three times more likely than the Industry Average and more than four times more likely than the Laggard class to have reduced infections from email in the last year

Laggard Steps to Success

Sixty-two percent of organizations in the Laggard Class suffered more lost productivity as a result of email than they did the year before. Compare this with the Best-in-Class of which 97% decreased lost productivity resulting from email.

Forty-two percent of the Laggard Class experienced an increase in the number of incidents of malware contracted from email compared with the Best-in-Class of which 84% decreased the number of incidents of malware contracted from email.

Twenty-one percent of the Laggard Class experienced an increase in the number of data loss incidents involving email while 65% experienced the same number as last year. Compare this with the fact that no Best-in-Class company experienced an increase in the number of data loss incidents, 29% remained the same as last year and 71% actually decreased the number of data loss incidents involving email.

As email threats continue to worsen, the consequences of failing to address these vulnerabilities put these organizations at greater and greater risk. Here are steps they should take immediately:

- Deploy a solution that constantly watches for the emergence of new threats and that automatically works to thwart them. Relying on users to update virus signatures or software leaves the user's machine vulnerable, and, if infected, threatens to infect others in the organization and those that communicate with the organization.
- Protect email in transmission – use some sort of encryption to protect the message itself.
- Deploy data loss prevention software that monitors outbound messages and attachments and can alert and intervene when email is being used inappropriately.
- Monitor and evaluate threats across the organization's resources.

Industry Average Steps to Success

Users in 66% of organizations in the Industry Average experienced some sort of malware infection on their desktops or laptops as the result of email. Twenty percent complain daily about spam. Twenty-eight percent lost more productivity as the result of email than the year previous. Without taking concrete steps to keep up with new and evolving threats, these organizations risk falling further and further behind. Here's where they should start:

- Deploy a solution to gain visibility into threats across all the organizations resources – desktops, laptops, servers and networks.
- Protect email in transmission – use some sort of encryption to protect the message itself.
- Deploy data loss prevention software that monitors outbound messages and attachments and can alert and intervene when email is being used inappropriately.
- Designate individual to review email abuse reports and quarantined mail.
- Measure productivity lost from email events to better understand the impact on the organization.

Best-in-Class Steps to Success

To stay ahead of the pack, Best-in-Class companies need to pay attention to the areas where email management needs to take a next step. They must:

- Define an enterprise-wide archive policy for email and implement it. Appropriate retention times will vary from industry to industry but Aberdeen research indicates that this area will be a subject of focus in the months to come.
- Develop a comprehensive messaging security strategy that addresses vulnerabilities in webmail, wikis, blogs, IM, chat and other messaging media where companies are beginning to experience susceptibility. Companies must prioritize based on the technologies actually used in their organizations.
- Insist on integration between email and web security, visibility into threats across the organizations resources, and a comprehensive email strategy that addresses both inbound and outbound vulnerabilities.

Aberdeen Insights – Summary

Using email is required – it's essential and business-critical for all organizations. Leaving an organization vulnerable because it uses email is *not* required, however – but unfortunately it is the case for most organizations. Because email is key to business but not the core business itself, organizations have traditionally paid it little heed. However, the risks associated with email rise daily. Organizations can no longer sit idly by waiting for someone else to take care of the problem.

Because email represents a threat on both the inbound and outbound side, a comprehensive strategy that addresses both sides of the exchange is necessary. The good news is that the organizations that are taking concrete actions can point to tangible improvement. Addressing email vulnerability has improved productivity, reduced cost and reduced risk.

Quote

"The ability to archive appropriately and thoroughly has become extremely important to us. We've developed a very clear policy and literal archive all email. Our counsel believes it's important that we have a copy of everything we receive and send and our industry requires we keep our archives for 7 years."

"It took us a couple of years to do this right, but everything is in place and works well. It serves as our backup operationally as well as what's necessary to meet compliance issues."

CIO of a billion-dollar Utility Company

Send to a Friend

Aberdeen Group
A Harte-Hanks Company

Appendix A: Research Methodology

Between June and July 2007, Aberdeen Group examined email vulnerabilities and strategies in more than 300 organizations.

Responding participants completed an online survey that included questions designed to determine the following:

- The extent to which organizations are effectively dealing with inbound email threats
- The extent to which organizations are effectively dealing with threats posed by outbound email
- The strategies, capabilities and technologies deployed to address these threats

Aberdeen supplemented this online survey effort with telephone interviews with select survey respondents, gathering additional information on email strategies, experiences, and results.

The study aimed to identify emerging best practices for email security and provide a framework by which readers could assess their own vulnerabilities.

Responding enterprises included the following:

- ***Job title/function:*** The research sample included respondents with the following job titles: senior management (CEO, COO, President), (20%), Manager (21%), Director (15%), CIO (14%), Staff (14%), Vice President (5%), Consultant (5%) and CFO (2%).
- ***Industry:*** The research sample included respondents from a cross section of industries. High Technology / software was the largest segment with 23% of the sample. Education accounted for 11% of respondents, Industrial equipment manufacturing (9%), telecommunication services (10%), and Finance / banking / accounting (8%).
- ***Geography:*** (60%) were from North America. Remaining respondents were from EMEA (Europe, Middle East and Africa) (21%), the Asia-Pacific region (17%) and other (2%).
- ***Company size:*** 17% of respondents were from large enterprises (annual revenues above US$1 billion); 29% were from midsize enterprises (annual revenues between $50 million and $1 billion); and 54% of respondents were from small businesses (annual revenues of $50 million or less).

Solution providers recognized as sponsors of this report were solicited after the fact and had no substantive influence on the direction of this report. Their sponsorship has made it possible for Aberdeen Group to make these findings available to readers at no charge.

Aberdeen Group
A Harte-Hanks Company

Table 4: PACE Framework

PACE Key
Aberdeen applies a methodology to benchmark research that evaluates the business pressures, actions, capabilities, and enablers (PACE) that indicate corporate behavior in specific business processes. These terms are defined as follows: ***Pressures*** **—** external forces that impact an organization's market position, competitiveness, or business operations (e.g., economic, political and regulatory, technology, changing customer preferences, competitive) ***Actions*** **—** the strategic approaches that an organization takes in response to industry pressures (e.g., align the corporate business model to leverage industry opportunities, such as product/service strategy, target markets, financial strategy, go-to-market, and sales strategy) ***Capabilities*** **—** the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products/services, ecosystem partners, financing) ***Enablers*** **—** the key functionality of technology solutions required to support the organization's enabling business practices (e.g., development platform, applications, network connectivity, user interface, training and support, partner interfaces, data cleansing, and management)

Table 5: Maturity Framework

Maturity Framework Key
The Aberdeen Maturity Framework defines enterprises as falling into one of the following three levels of practices and performance: ***Best-in-Class (20%)*** **—** Organizations that demonstrate the secure email practices that are the best currently being employed and significantly superior to the industry norm, and result in the top industry performance. ***Industry norm (50%)*** **—** Organizations that demonstrate the secure email practices that represent the average or norm, and result in average industry performance. ***Laggards (30%)*** **—** Organizations that demonstrate the secure email practices that are significantly behind the average of the industry, and result in below average performance In the following categories: ***Process*** **—** What is the scope of process standardization? What is the efficiency and effectiveness of this process? ***Organization*** **—** How is your company currently organized to manage and optimize this particular process? ***Knowledge*** **—** What visibility do you have into key data and intelligence required to manage this process? ***Technology*** **—** What level of automation have you used to support this process? How is this automation integrated and aligned? ***Performance*** **—** What do you measure? How frequently? What's your actual performance?

Source: Aberdeen Group, July 2007

Table 6: Relationship between PACE and Competitive Framework

PACE and Competitive Framework How They Interact
Aberdeen research indicates that companies that identify the most impactful pressures and take the most transformational and effective actions are most likely to achieve superior performance. The level of competitive performance that a company achieves is strongly determined by the PACE choices that they make and how well they execute.

Source: Aberdeen Group, July 2007

Aberdeen Group
A Harte-Hanks Company

Appendix B:
Related Aberdeen Research

Related Aberdeen research that forms a companion or reference to this report includes:

Thwarting Data Loss, May 2007.

Information on these and any other Aberdeen publications can be found at www.Aberdeen.com.

Author: Carol Baroudi, Research Director, IT Security (*Carol.Baroudi@aberdeen.com*)