

## **Safe Email**

Seven Important Tips for  
Better Email Security in 2009

June 2009

Carol Baroudi





## Safe Email Seven Important Tips for Better Email Security in 2009

Google is happy to provide you with this Aberdeen Group research paper that will help you in evaluating how cloud computing security solutions can benefit your business.

As many of the Best-in-Class organizations featured in this report know, cloud computing offers effective solutions that improve security while reducing cost and the complexity of your IT infrastructure.

Google security and archiving services, powered by Postini, are cloud computing solutions that make email systems more secure, compliant and productive by blocking spam and other intrusions before they reach your network, and by providing encryption and archiving to help you meet compliance requirements.

For more information about Postini services and the full line of Google Apps solutions for businesses and organizations, please visit:  
<http://www.google.com/postini>.



Your complimentary access to this *Aberdeen Group* report is made possible through a special distribution license granted to Google, Inc. *Aberdeen Group* bears sole responsibility for the research findings and analysis included in this report. The findings and views expressed in this report do not necessarily reflect the views of the licensee.

## Executive Summary

Well-financed email threat creators persist in propagating ever more sophisticated and potentially lethal attacks through the estimated 62 trillion spam messages sent last year. Stressful economic times strain budgets and the staff responsible for email security. Growing numbers of *former* employees leave their former *employers* at higher risk. Add the rising value of sensitive data in a desperate market, and we have a set of trends that all point to critical reasons organizations cannot ignore their email vulnerabilities. This report highlights ways Best-in-Class organizations harden themselves against threats from email.

### Research Benchmark

Aberdeen's Research Benchmarks provide an in-depth and comprehensive look into process, procedure, methodologies, and technologies with best practice identification and actionable recommendations.

### Best-in-Class Performance

---

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

- Reduced lost productivity as a result of email
- Decreased volume of spam reaching end-users
- Decreased cost associated with recovery from email attacks
- Decreased data loss incidents attributable to email
- Decreased number of incidents of viruses, Trojans, spyware, and botnet or other malware infections contracted from email

### Competitive Maturity Assessment

---

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

- 58% reduced the number of incidents of email attacks targeted at individuals
- 54% reduced lost business, lost productivity, or lost information as a result of false positives
- 38% reduced financial loss from data loss as a result of email-related events (including fraud)

### Recommended Actions

---

In addition to the specific recommendations in Chapter Three of this report, users should:

- Create a comprehensive email security strategy that includes inbound and outbound email, and email internal to the organization
- Define and enforce consistent email and data security policies
- Educate users on safe and appropriate email use

“We’re an international firm and we’ve had the horrible experiences of seeing our competitors with exact duplicates of our emailed proposals in their hands. We’ve found a way to ensure that our targeted recipient and only our targeted recipient gets what we’re sending and we’re very happy. We’ve been doing this since the first of the year and aren’t experiencing any of the problems we experienced before. We also need to transmit large architectural drawings as well as large medical digital imaging files. This is proving to be a much better way for us to exchange data.”

~ CEO, \$5 million international consulting firm

## Table of Contents

---

Executive Summary.....	2
Best-in-Class Performance.....	2
Competitive Maturity Assessment.....	2
Recommended Actions.....	2
Chapter One: Benchmarking the Best-in-Class .....	4
Business Context .....	4
The Maturity Class Framework.....	4
The Best-in-Class PACE Model .....	5
Best-in-Class Strategies.....	6
Chapter Two: Benchmarking Requirements for Success .....	8
Competitive Assessment.....	8
Capabilities and Enablers.....	9
Chapter Three: Recommended Actions .....	12
Laggard Steps to Success.....	12
Industry Average Steps to Success .....	12
Best-in-Class Steps to Success.....	13
Appendix A: Research Methodology.....	15
Appendix B: Related Aberdeen Research.....	17

## Figures

---

Figure 1: Top Reasons Organizations Focus on Email Security .....	4
Figure 2: Year over Year Best-in-Class Security Strategies .....	6

## Tables

---

Table 1: Top Performers Earn Best-in-Class Status.....	4
Table 2: The Best-in-Class PACE Framework .....	5
Table 3: The Competitive Framework.....	9
Table 4: Technology Enablers Adoptions by Class .....	11
Table 5: The PACE Framework Key .....	16
Table 6: The Competitive Framework Key .....	16
Table 7: The Relationship Between PACE and the Competitive Framework .....	16

## Chapter One: Benchmarking the Best-in-Class

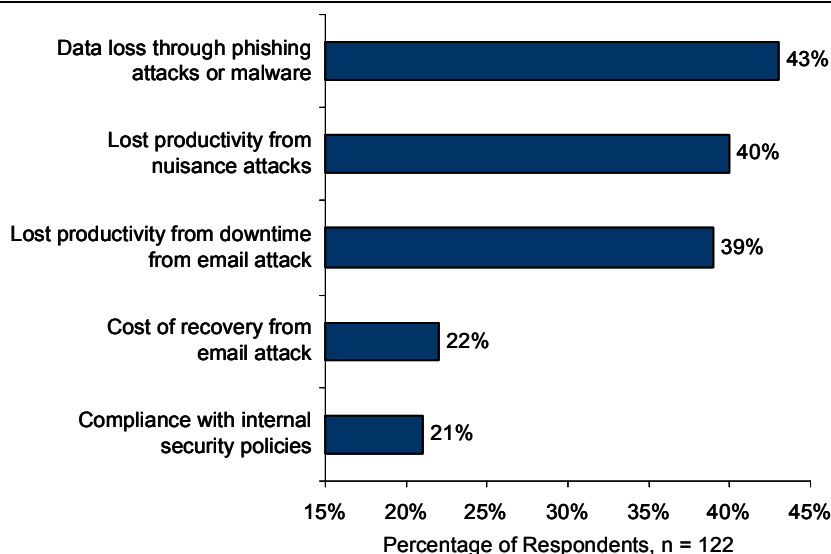
### Business Context

Email — organizations can't live without it and it puts every organization at risk. As a global enabler of communications and collaboration, email simultaneously is the medium of choice for many hackers worldwide. Left unattended, email vulnerabilities can cripple an organization and devastate its brand. Solutions abound, but root causes – malware laden spam, email with links to malicious web sites, phishing attempts, intentional and unintended data loss, botnet infestations – persist unabated, growing ever more clever and ever more resistant to detection. This year's Aberdeen research indicates organizations are driven to focus on email security by the need to protect themselves from the damages email attacks can cause.

#### Fast Facts

- ✓ **42%** of the Best-in-Class decreased their help-desk costs and time need to remediate email attacks by more than 20%
- ✓ **34%** of the Best-in-Class decreased the number of incidents of non-compliance with regulations

**Figure 1: Top Reasons Organizations Focus on Email Security**



Source: Aberdeen Group, May 2009

### The Maturity Class Framework

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

**Table 1: Top Performers Earn Best-in-Class Status**

Definition of Maturity Class	Mean Class Performance
<b>Best-in-Class: Top 20%</b> of aggregate performance scorers	<ul style="list-style-type: none"> <li>▪ 10% improvement in lost productivity as a result of email over past 12 months</li> <li>▪ 17% decrease in volume of spam reaching user inboxes over past 12 months</li> <li>▪ 11% decrease in total cost associated with recovery from email attacks over past 12 months</li> <li>▪ 5% decrease in incidence of data loss associated with email over past 12 months</li> <li>▪ 11% decrease in incidence of malware contracted from email over past 12 months</li> </ul>

Definition of Maturity Class	Mean Class Performance
<b>Industry Average: Middle 50%</b> of aggregate performance scorers	<ul style="list-style-type: none"> <li>▪ No change in productivity as a result of email</li> <li>▪ 1% decrease in volume of spam reaching user inboxes over past 12 months</li> <li>▪ 1% increase in total cost associated with recovery from email attacks over past 12 months</li> <li>▪ No change in number of data loss incidents associated with email over past 12 months</li> <li>▪ No change in incidence of malware contracted from email over past 12 months</li> </ul>
<b>Laggard: Bottom 30%</b> of aggregate performance scorers	<ul style="list-style-type: none"> <li>▪ 7% increase in lost productivity as a result of email</li> <li>▪ 8% increase in volume of spam reaching user inboxes over past 12 months</li> <li>▪ 5% increase in total cost associated with recovery from email attacks over past 12 months</li> <li>▪ 6% increase in number of data loss incidents associated with email over past 12 months</li> <li>▪ 5% increase in incidence of malware contracted from email over past 12 months</li> </ul>

Source: Aberdeen Group, May 2009

## The Best-in-Class PACE Model

Creating an effective email security strategy requires a combination of strategic actions, organizational capabilities, and enabling technologies. Like other aspects of IT security, email security is best addressed in layers of solutions that work together to create a robust defense.

Email security must consider three fundamental dimensions of vulnerability:

- **Inbound email threats** such as spam, phishing attacks, malware, spyware, blended threats, scams, and spoofs.
- **Outbound vulnerabilities and liabilities** including accidental data loss, intentional data leakage, botnet activity, and contaminated outbound mail. Outbound protection strategies must protect email in transit.
- **Risks associated with email within the organization** including inappropriate sharing of sensitive data and malware contamination. Organizations must protect email "at rest" – both the contents of user inboxes and folders as well as email archives.

**Table 2: The Best-in-Class PACE Framework**

Pressures	Actions	Capabilities	Enablers
<ul style="list-style-type: none"> <li>▪ Lost productivity from nuisance attacks (i.e., innocuous spam)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Protect users from unwanted email and inbound email vulnerabilities</li> <li>▪ Prevent the dissemination of spam or infected email from the organization</li> </ul>	<ul style="list-style-type: none"> <li>▪ Identification and response to threats in automated manner</li> <li>▪ Individual or group responsible for reviewing email abuse reports</li> <li>▪ Instantaneous, automatic update of threat protection</li> <li>▪ Email use reports</li> </ul>	<ul style="list-style-type: none"> <li>▪ Virus, worm, Trojan protection</li> <li>▪ Anti-spoofing, anti-phishing, anti-spyware, anti-key logger, anti-fraud</li> <li>▪ Defined email policy</li> <li>▪ Attachment filtering</li> <li>▪ Integrated email and Internet security</li> <li>▪ Email security in the cloud from a service provider</li> </ul>

Source: Aberdeen Group, May 2009

## Best-in-Class Strategies

Best-in-Class organizations put their primary focus on:

- Protecting users from unwanted email and inbound email vulnerabilities
- Preventing the dissemination of spam or infected email from the organization
- Training employees in email best practices

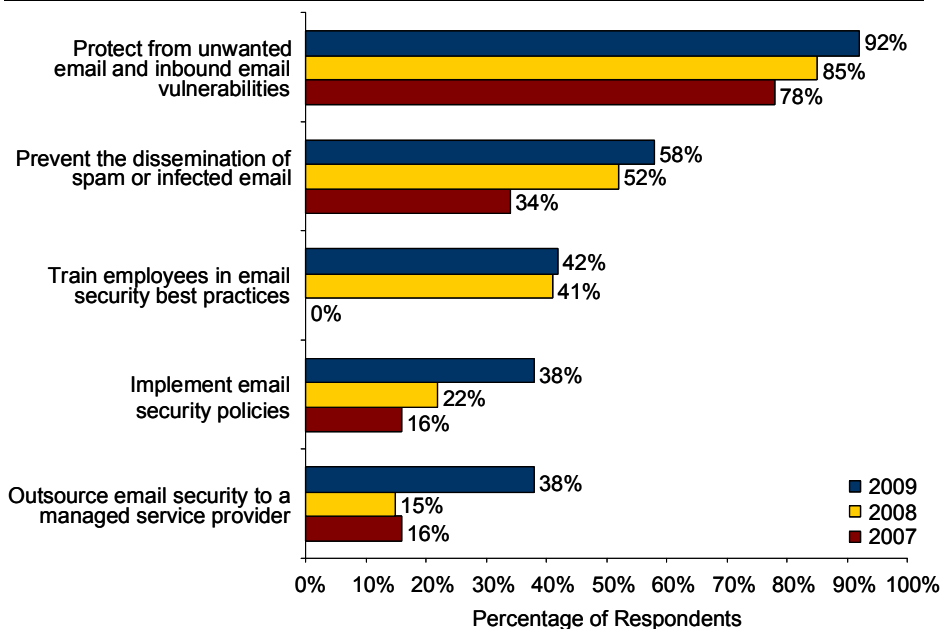
Each of these areas of focus needs to be kept current. New and more sophisticated email threats arise continuously and must be dealt with by both keeping email protection capabilities at a state of the art level, and by keeping employees up-to-date with the latest forms of phishing and social engineering, email acceptable use policies, and pertinent regulations that apply to their email use.

Year over year, Best-in-Class organizations are putting more focus on email security policies and are more often viewing outsourcing email security as a strategy to achieve their goals. Outsourcing email security goes by many names, such as Security in the Cloud, Managed Security Services, or Security- (or Software-) as-a-Service, to name the most common. Choosing to outsource email security as a top strategy is up more than 150%.

"We've had only one email breach in the last two years and have pretty much eliminated spam. I'd say that's pretty good. I'm downgrading one of our appliances because it's redundant to the functionality I'm getting from another solution. We've added a hundred users in the last few months, but not everybody has their own computer, so I have to make sure that webmail is safe too."

~ IT Manager, US County Government

**Figure 2: Year over Year Best-in-Class Security Strategies**



Source: Aberdeen Group, May 2009

### Aberdeen Insights — Strategy Tips

In considering email security strategy it's critical you pay attention to two important areas:

**1. Consider email security from all angles.** First, you must address incoming email and the potential threats it may carry including contaminated mail carrying malware, phishing attacks, and pieces of a blended threat – innocuous seeming email that has a dangerous link inside. Second, you must address your outbound mail security, including protecting legitimate mail in transit, preventing both intentional and unintended data leakage, and making sure email from your organization is free from malware. In addition you must monitor for botnet activity, as it may originate from infected machines in your organization without your knowledge unless you're actively trying to detect it. Third, you must look at email internal to your organization – computers can get infected many ways and you don't want to spread contamination within your organization. Likewise, you don't want sensitive data leaked to someone within the organization who does not have legitimate access to it.

**2. Critical to your overall success is defining and enforcing email security policies,** including explicit rules around handling sensitive data. You are responsible for your organization's sensitive data and virtually everyone has access to email. If you're not protecting your data vis-à-vis its inclusion in email messages or attachments, you're not protecting your data.

In the next chapter, we look at what top performers are doing to achieve these results.

## Chapter Two: Benchmarking Requirements for Success

The selection of email security solutions plays a crucial role in the ability to achieve strong security.

### Case Study —Municipal Government – US City

The Chief Technology Officer for a mid-size US city says that they are primarily concerned about threats coming from the outside. They use an Intrusion Detection System to protect their network in general, as well as using Network Access Control, and penetration testing.

They are concerned about loss of productivity from email viruses and spam, and cost is of concern, but not the primary driver. They began using a hosted anti-spam solution and are very happy with it. In addition, they've begun experimenting with web security hosting from a separate provider that does content filtering. As yet, these two solutions are not integrated.

Because the city is a public entity that is accountable in investigations, they've chosen to adopt more stringent practices than they think they may need. "We can't keep up with everything we're supposed to. We don't have security experts on staff. We can't keep up-to-date," the CTO explains. Rather than risk being held accountable, should they have some sort of security event, they've chosen to outsource much of their IT security.

The city's IT department is responsible for 1,200 computers and is prepared to change vendors / providers as more robust and cost-cutting solutions become available.

### Fast Facts

- √ Best-in-Class organizations are **54%** more likely than all other respondents to verify the email sender's authenticity
- √ Best-in-Class organizations are **67%** more likely than Laggard organizations to monitor outbound traffic for botnet activity

### Competitive Assessment

Aberdeen Group analyzed the aggregated metrics of surveyed companies to determine whether their performance ranked as 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 approaches they take to execute their daily operations); (2) **organization** (corporate focus and collaboration among stakeholders); (3) **knowledge management** (contextualizing data and exposing it to key stakeholders); (4) **technology** (the selection of appropriate tools and effective deployment of those tools); and (5) **performance management** (the ability of the organization to measure its results to improve its business). These characteristics (identified in Table 3) serve as a guideline for best practices, and correlate directly with Best-in-Class performance across the key metrics.

**Table 3: The Competitive Framework**

	Best-in-Class	Average	Laggards
<b>Process</b>	Defined email policy:		
	79%	70%	65%
<b>Organization</b>	End-user training in safe email practice:		
	67%	48%	47%
	Individual responsible for reviewing email abuse reports:		
	83%	58%	55%
<b>Knowledge</b>	Email use reports:		
	75%	52%	35%
<b>Technology Integration</b>	Integrated email and Internet security:		
	71%	55%	39%
<b>Performance</b>	Email Threat Reports:		
	75%	52%	35%

Source: Aberdeen Group, May 2009

## Capabilities and Enablers

Best-in-Class organizations align themselves in support of security measures through their processes, organizational roles, use of reports, use of technology enablers, and measurement of their own performance. Aberdeen analysis indicates that they use the following capabilities and enablers to a greater extent than the classes.

### Process

Training end-users in safe email practice requires continuous re-enforcement and updating to keep users aware of the latest dupes designed with very sophisticated socially engineered tactics. This year, for example, end-users need to be alerted to the fact that newer phishing attacks are designed to look as if they are coming from someone within the organization itself. Some are addressed to colleagues with the recipient cc'd or bcc'd. Alerting end-users to known new threats can minimize the chances that they'll be conned into opening such mail.

### Organization

Organizations need to create email abuse reports and they need someone knowledgeable whose job includes reviewing the reports to detect attempted abuse as well as identify the target of such attempts. Creating the reports alone does nothing unless someone who knows what they mean reviews them regularly.

### Knowledge Management

Creating email use reports is critical to designing and implementing appropriate email security policies. Understanding the organization's norm helps identify abnormal behaviors.

“Our current spam filter does not work and we're actively looking to replace it. I know we shouldn't be getting this kind of volume of spam.”

~ CFO, Travel and Entertainment Association

## Technology

Organizations need to **scan incoming mail for all sorts of malware** – keep whatever you can outside. They need to scan all outgoing mail as well, because computers can get infected by visiting malicious sites, or introducing infections by way of contaminated files from a thumb drive, CD, or DVD. Don't risk contaminating others in the organization or damaging the organization's brand by sending out malware-laden email. Overall email security relies in part on endpoint security. Despite what everyone agrees is best practice, not all organizations insist on protecting their endpoints, and that's a mistake.

Beyond traditional anti-virus protection, organizations need to **explicitly work to deter phishing attacks**, the installation of spyware and key loggers, and work to thwart fraud. The escalation of attacks through email continues to rise unabated and you can expect this trend to perpetuate indefinitely. It's critical that organizations find ways to keep current in the email threat domain.

**Policy** is key to protecting the organization and its data. Email security policies can be refined over time, but begin by establishing and enforcing policy now.

**Email attachments** can be problematic on several fronts – they must be **scanned to ensure they don't contain malware, and they must be scanned to prevent inadvertent data loss.**

Many threats come in a form known as a **blended threat**. In a blended threat, innocuous looking email – email that is not obviously spam – contains a link that resolves to a malicious site. As new malicious sites arise at every moment, organizations need a **tight coupling between their email security and their web security**. Some anti-spam solutions actually check each link inside an email to determine if the sites where they point are legitimate.

**Data loss** tops the list of biggest concerns across all respondents, yet most organizations have yet to explicitly address data loss. **Identifying sensitive data and creating policies to protect it** are critical to preventing data loss.

**Highly sensitive data may call for special handling.** Certain data may be so sensitive that you may want to keep it out of the traditional flow of email, period. Because traditional email follows well-defined protocols and paths for delivery, it's subject to attacks designed to exploit known vulnerabilities and common email use. Availing yourself a completely separate secure channel for communication might prove the safer course of action for information considered highly sensitive – government security data, patient healthcare data, and financial transactions, for example.

"Phishing is still a big concern for me for our end-users, although, with changes we've made this year, we're definitely seeing less. I'm still concerned about email that's showing up in our inboxes that looks like it came from inside the organization – it's a tough thing to explain to people why email seems to be coming from themselves. I used to try to manage all email security in-house, but we switched to using email security services and it's quite a relief."

~ VP, Customer Service,  
Virginia-based Small  
Business

**Table 4: Technology Enablers Adoptions by Class**

Technology Enabler	Best-in-Class	Industry Average	Laggards
Anti-spoofing, anti-phishing, anti-spyware, anti-key logger, anti-fraud	83%	66%	61%
Integrated email and Internet security	71%	55%	50%
Data loss prevention solution	42%	36%	23%
Scan attachments for sensitive data	42%	29%	17%
Attachment filtering for malware	71%	58%	50%
Virus, worm, Trojan protection	100%	88%	74%

Source: Aberdeen Group May 2009

**Performance Management**

Awareness and understanding of the email threats reaching the organization is critical to the continual refinement of email security policies and the bolstering of support where it's most needed.

**Aberdeen Insights — Technology Tips**

- 3. Zero Hour Protection** – New email threats emerge perpetually. Labs work 24 / 7 to identify new threats and protect against them. You should avail yourself of these protections the instant they become available. It's no wonder that Best-in-Class organizations automatically respond to new threats to a much greater extent than the other classes, and most Best-in-Class organizations have protection in place for new threats within a few hours. Organizations that update their email protection on a scheduled basis rather than when the protection becomes available leave themselves needlessly vulnerable and, as our data indicates, suffer many more incidents of downtime and data loss.
- 4. Reputation** – Detecting and deflecting spam is a science unto itself. One key element is understanding where the spam actually originates – what's the reputation of the sender. Various vendors approach this issue of reputation differently, but Best-in-Class organizations are 54% more likely to verify the authenticity of the sender than other organizations.
- 5. Encryption** – Protecting email in transmission is critical to protecting sensitive data. Coupled with data loss solutions that either prevent unencrypted sensitive data from being sent or automatically encrypt sensitive data to protect it, organizations can take a big step in preventing data loss. Part of end-user training must be a reminder that email sent in the clear is like sending mail on a postcard – everyone who sees it can read it. Also, part of end-user training must be conveying the fact that technology exists that is actively looking at traffic to detect and collect sensitive data such as credit card numbers and social security numbers. Would-be villains don't need to know their victims – they simply prey on the unprotected.

## Chapter Three: Recommended 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, the following actions will help spur the necessary performance improvements:

### Laggard Steps to Success

---

- **Implement anti-virus, -worm, -Trojan, -malware protection.** All (100%) of the Best-in-Class have done this, while only 74% of Laggards have. This is a “must-have” for every computer in every organization. No exceptions.
- **Train end-users in safe email practices.** In an ideal world technology would thwart every attack and catch every data breach. However, as new attacks are being invented at every moment, keeping end-users aware of current threats minimizes the likelihood of their falling prey to the latest trap. Likewise, often it's uneducated users who send sensitive data inappropriately only because they don't know they shouldn't; implementing end-user training is imperative. Only 47% of Laggard organizations provide training in safe email practices versus 67% of Best-in-Class organizations.
- **Implement a data loss prevention strategy.** Only 23% of the Laggards implements data loss prevention, compared with 42% of the Best-in-Class. As the Laggards cite fear of data loss as a top driver for their focus on email security, making strides toward actual data loss prevention is a good place to start.

### Industry Average Steps to Success

---

- **Filter email attachments for malware.** Only 58% of the Industry Average filter their email attachments for malware, versus 71% of the Best-in-Class. Email attachments are known to harbor malicious code, and scanning email attachments as well as the body of the email is critical.
- **Integrate email and web security.** Because most of today's threats are blended threats – that is, threats that may begin with a seemingly innocuous email containing a URL that points to a malicious site – end-users need either email scanning that actually evaluates all embedded links, checking the sites to which they point, or they need tightly coupled web security that will prevent a link they click on in an email from resolving at a contaminated site. Ideally, they never have to see such mail in the first place.
- **Implement anti-phishing, anti-spyware, anti-key logging, anti-fraud solutions.** Increasingly sophisticated phishing attacks are of major concern, and data loss through these attacks is of

### Fast Facts

- √ 54% of Best-in-Class organizations were able to reduce lost business, lost productivity, or lost information as a result of false positives.
- √ 38% of Best-in-Class organizations were able to reduce financial loss due to data lost through email-related events, including fraud.

“We did make a switch in our email strategy and found we have a much better handle on threats and it's a lot easier to manage.”

~ IT Manager, Large Health Care Provider, Southwest US

primary concern to most respondents. Many of these threats can be detected and thwarted with appropriate solutions.

## Best-in-Class Steps to Success

- **Leverage the cloud.** Using either a cloud-based solution or a hybrid solution that leverages the cloud, include cloud-based email security to ensure that spam and email threats that can be eliminated outside your network stay outside your network. Keeping known spam and infected mail outside lowers your risk and saves the potential costs of archiving unwanted mail.
- **Scan outbound email attachments for sensitive data.** Data in spreadsheets, word documents, PowerPoint presentations, and patient records, may well be data sensitive to the organization or protected by data privacy legislation. Without actively scanning outbound attachments, organizations leave themselves vulnerable to data leakage and regulatory sanction.
- **Obtain data use reports.** To protect their data, organizations need to classify their data and implement policies that limit access to sensitive data. To understand how data is being used within the organization requires data use reports. Email security policies that protect the organization while maintaining flexibility require knowledge of who has legitimate access to what data.

### Aberdeen Insights — Summary

Protecting the organization and its data from the threats posed by email requires constant vigilance and enforcement – awareness of new threats as they emerge, an understanding of the organization's sensitive data and how to protect it, and an understanding that email is a mission-critical application that creates a backbone of communication within the organization and with customers, business partners, and prospects. Loss of the ability to send and receive email (email availability) can prove damaging if not disastrous depending on the length of outage and the business processes that rely on email.

Deploying many elements of email security in the cloud is proving an ever more attractive option for many organizations – note the increase in Chapter One. Reasons organizations consider this strategy include:

- Leveraging the ability to detect threats across customers and across networks and stop email threats before they enter the organization's network
- Leaving the security expertise to organizations whose job it is to focus on security 24 / 7
- Freeing the organization's staff to focus on its line of business

*continued*

### Aberdeen Insights — Summary

- Shifting from capital expenditure to operational expenditure

End-users to whom we spoke said that their organizations' ability to address the spectrum of security threats is inadequate and they are availing themselves of outside services to bridge the gap.

In considering overall email security, organizations need to expand their view to encompass two more elements:

**6. Maintaining the availability of email** – eliminating downtime and outages that can leave the organization crippled without this mission critical application.

**7. Protecting the email itself through appropriately protected email archiving.** Archiving is critical to business continuity as well as to protecting the organization should the need arise for e-discovery.

Email security is a must-have. And up-to-date email security, security ready to contend with threats as they emerge, can spare the organization lost productivity, lost business, and the costs associated with email attacks.

## Appendix A: Research Methodology

Between April and May 2009, Aberdeen examined the use, the experiences, and the intentions of more than 130 organizations using email security.

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

Responding enterprises included the following:

- *Job title / function:* The research sample included respondents with the following job titles: IT manager or staff (67%); senior management (24%); consultant / other (9%).
- *Industry:* Respondents came from dozens of different industries including High technology / software (19%), Education (10%), Telecommunications (9%), and Finance / Banking / Accounting (8%).
- *Geography:* The majority of respondents (62%) were from North America. Remaining respondents were from the Asia-Pacific region (19%) and EMEA (19%).
- *Company size:* Fifteen percent (15%) of respondents were from large enterprises (annual revenues above US \$1 billion); 24% were from midsize enterprises (annual revenues between \$50 million and \$1 billion); and 61% of respondents were from small businesses (annual revenues of \$50 million or less).
- *Headcount:* Fifty-two percent (52%) of respondents were from large enterprises (headcount between 1 and 99 employees); 18% were from midsize enterprises (headcount between 100 and 999 employees); and 30% of respondents were from small businesses (headcount greater than 1,000 employees).

Solution providers recognized as sponsors 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.

### Study Focus

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

- √ The degree to which email security is deployed in their operations and the manner in which it is deployed
- √ The effectiveness of existing email security implementations
- √ Current and planned use of email security
- √ The benefits of deploying email security

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

**Table 5: The PACE Framework Key**

Overview
<p>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:</p> <p><b>Pressures</b> — external forces that impact an organization’s market position, competitiveness, or business operations (e.g., economic, political and regulatory, technology, changing customer preferences, competitive)</p> <p><b>Actions</b> — 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)</p> <p><b>Capabilities</b> — the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products / services, ecosystem partners, financing)</p> <p><b>Enablers</b> — 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)</p>

Source: Aberdeen Group, May 2009

**Table 6: The Competitive Framework Key**

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

Source: Aberdeen Group, May 2009

**Table 7: The Relationship Between PACE and the Competitive Framework**

PACE and the Competitive Framework – How They Interact
<p>Aberdeen research indicates that companies that identify the most influential 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 those decisions.</p>

Source: Aberdeen Group, May 2009

## Appendix B: Related Aberdeen Research

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

- [\*The 2008 Email Security Report\*](#); August 2008
- [\*Education Sector "Left Behind" When it Comes to Email Security\*](#); October 2008
- [\*Public Sector Hugs the Middle of the Road in Email Security\*](#); October 2008
- [\*Data Loss Prevention: Little Leaks Sink the Ship\*](#); June 2008
- [\*Best Practices in Choosing and Managing Security Services\*](#); January 2008
- [\*The Ins and Outs of Email Vulnerabilities\*](#); July 2007
- [\*Thwarting Data Loss\*](#); May 2007
- [\*Educational Institutions Need to Get Smarter about Email Security\*](#); December 2007

Information on these and any other Aberdeen publications can be found at [www.aberdeen.com](http://www.aberdeen.com).

Author: Carol Baroudi, Research Director, IT Security  
[carol.baroudi@aberdeen.com](mailto:carol.baroudi@aberdeen.com)

Since 1988, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.2 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen plays a key role of putting content in context for the global direct and targeted marketing company. Aberdeen's analytical and independent view of the "customer optimization" process of Harte-Hanks (Information – Opportunity – Insight – Engagement – Interaction) extends the client value and accentuates the strategic role Harte-Hanks brings to the market. For additional information, visit Aberdeen <http://www.aberdeen.com> or call (617) 723-7890, or to learn more about Harte-Hanks, call (800) 456-9748 or go to <http://www.harte-hanks.com>.

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc.