

The 2008 Email Security Report

Combating Spam, Data Loss, Fraud, Zombies, Non-Compliance and Sabotage

August 2008

Executive Summary

Every organization depends on email - and unfortunately, email vulnerabilities perpetually plague email administrators and users alike. Malicious email threatens information security, overall system security, and user productivity. Phishing and individually target attacks are on the rise. Outbound email can be a vehicle for data loss, spreading malware and spam, and denial of service attacks. Inappropriate email within an organization may challenge regulatory compliance and data security.

In the course of the year, the volume and effectiveness of malicious email continues to increase dramatically, bringing down ISPs, stealing sensitive data, and leaving millions of compromised machines undetected, unwittingly under the control anonymous perpetrators. Data loss solutions are more widely adopted, and organizations are actively changing email strategy to try to gain better control and manageability around email security.

Best-in-Class Performance

Aberdeen used five key performance criteria to distinguish Best-in-Class companies. As a class these organizations significantly

- Reduced lost productivity as a result of email
- Decreased the volume of spam reaching end users
- Decreased the cost associated with recovery from email attacks
- Decreased data loss incidents attributable to email
- Decreased the number of incidents of viruses, Trojans, spyware, 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:

- 45% reduced lost business, lost productivity, or lost information as a result of false positives
- 41% reduced help desk time / cost of remediating email attacks
- 34% reduced non-compliance associated with email or data in email

Required Actions

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

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

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

"We had no reason to suspect we had a problem with botnets. Then suddenly we were caught in a horrible cycle of huge quantities of mail being returned as undeliverable. We didn't know the source. The standard log files were useless. There was no granular way to really track what was going on. Our software was unequipped to handle non-delivery messages had no way to specify specific actions for particular cases. These attacks were bringing all of our systems down every two hours. We were quite desperate for help - and fortunately we found it."

~ Server Operations Manager,
Leading International ISP and
Systems Integrator

Table of Contents

Executive Summary.....	2
Best-in-Class Performance.....	2
Competitive Maturity Assessment.....	2
Required Actions.....	2
Chapter One: Benchmarking the Best-in-Class	4
Business Context	4
The Maturity Class Framework.....	5
The Best-in-Class PACE Model	6
Best-in-Class Strategies.....	7
Chapter Two: Benchmarking Requirements for Success	9
Competitive Assessment.....	10
Capabilities and Enablers.....	12
Chapter Three: Required Actions	15
Laggard Steps to Success.....	15
Industry Average Steps to Success	16
Best-in-Class Steps to Success.....	17
Appendix A: Research Methodology.....	19
Appendix B: Related Aberdeen Research.....	21
Featured Underwriters	Error! Bookmark not defined.

Figures

Figure 1: Top Pressures Driving Organizations' Focus on Email Security.....	4
Figure 2: Best-in-Class Strategies for Email Security	7

Tables

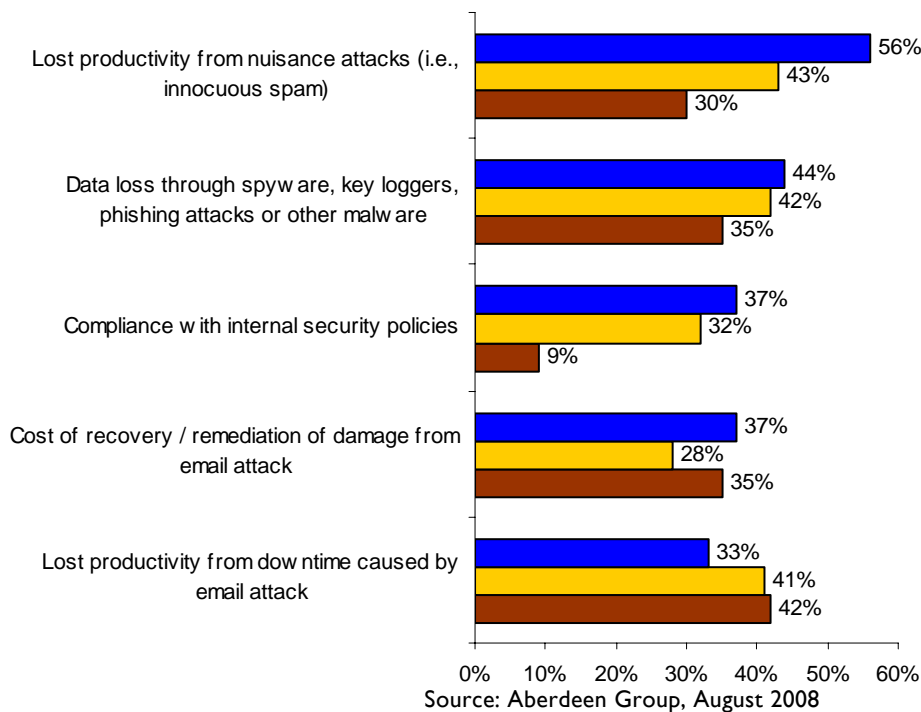
Table 1: Top Performers Earn Best-in-Class Status.....	5
Table 2: The Best-in-Class PACE Framework	6
Table 3: The Competitive Framework.....	10
Table 4: The PACE Framework Key	20
Table 5: The Competitive Framework Key	20
Table 6: The Relationship Between PACE and the Competitive Framework	20

Chapter One: Benchmarking the Best-in-Class

Business Context

Widely touted as a critical productivity tool, email is also central to business communications. However, email exposes organizations to serious vulnerability and liability - and protecting an organization's data, infrastructure, and brand requires a well-considered strategy and ongoing vigilance.

Figure 1: Top Pressures Driving Organizations' Focus on Email Security



Fast Facts

- ✓ 67% of Best-in-Class organizations respond to new email threats in less than an hour
- ✓ 56% of Best-in-Class companies reduced help desk time and the cost of remediation of email infections

New exploits that leverage email's inherent vulnerabilities surface constantly, necessitating an email security strategy that perpetually contends with emerging threats in a timely way. Botnet attacks which are responsible for most spam, last only a few hours. Failure to react to new attacks in a timely way leaves organizations highly vulnerable.

Because email is woven into business processes, creating sound email security means looking closely at work flows and dependencies. Securing email and the data contained in email is not simple. For organizations contending with regulatory compliance such as financial services and health care, ensuring email security means identifying every route email travels, mapping access to sensitive data against data use policies, and ensuring that sensitive data is delivered only to those with legitimate access.

The Maturity Class Framework

Aberdeen used five key performance criteria to distinguish the Best-in-Class from Industry Average and Laggard organizations (Table 1).

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

Definition of Maturity Class	Mean Class Performance
<p>Best-in-Class: Top 20% of aggregate performance scorers</p>	<ul style="list-style-type: none"> ▪ 22% reduced lost productivity as a result of email (spam and infection) by more than 20% ▪ 67% decreased the volume of spam reaching end user inboxes by more than 20% ▪ 26% decreased the total cost associated with recovery from and remediation of email attacks by more than 20% ▪ 42% decreased the number of data loss incidents attributable to email ▪ 37% decreased the number of incidents of viruses, Trojans, spyware, botnet or other malware infections contracted from email by more than 20%
<p>Industry Average: Middle 50% of aggregate performance scorers</p>	<ul style="list-style-type: none"> ▪ 3% reduced lost productivity as a result of email (spam and infection) by more than 20% ▪ 11% decreased the volume of spam reaching end user inboxes by more than 20% ▪ 0% decreased the total cost associated with recovery from and remediation of email attacks by more than 20% ▪ 9% decreased the number of data loss incidents attributable to email ▪ 3% decreased the number of incidents of viruses, Trojans, spyware, botnet or other malware infections contracted from email by more than 20%
<p>Laggard: Bottom 30% of aggregate performance scorers</p>	<ul style="list-style-type: none"> ▪ 0% reduced lost productivity as a result of email (spam and infection) by more than 20% ▪ 4% decreased the volume of spam reaching end user inboxes by more than 20% ▪ 0% decreased the total cost associated with recovery from and remediation of email attacks by more than 20% ▪ 0% decreased the number of data loss incidents attributable to email ▪ 0% decreased the number of incidents of viruses, Trojans, spyware, botnet or other malware infections contracted from email by more than 20%

Source: Aberdeen Group, August 2008

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

Table 2: The Best-in-Class PACE Framework

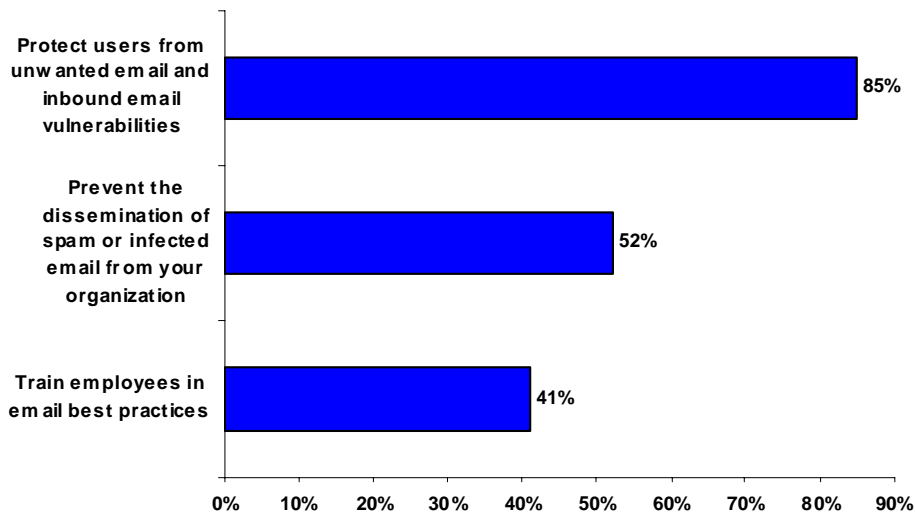
Pressures	Actions	Capabilities	Enablers
<ul style="list-style-type: none"> ▪ Lost productivity from nuisance attacks (SPAM) 	<ul style="list-style-type: none"> ▪ Protect users from unwanted email and inbound email vulnerabilities ▪ Prevent the dissemination of spam or infected email from the organization ▪ Train employees in email best practices 	<ul style="list-style-type: none"> ▪ Role-based email security policy ▪ Inbound email protection ▪ Verification of email sender's authenticity ▪ Protection of email in transmission ▪ Monitor outbound traffic for botnet activity ▪ Scan email attachments for sensitive data ▪ Identify and respond to new threats in a timely and automated way ▪ Integrated email and web security ▪ Protection for web mail ▪ User training in safe email practices ▪ Individual responsible for reviewing email abuse reports ▪ Individual responsible for evaluating inbound email in quarantine ▪ Real-time notification of inappropriate email use ▪ Email acceptable use policy ▪ Automated enforcement of acceptable use policy ▪ Data use reports ▪ Email usage reports ▪ Email threat reports ▪ Track fraud from email ▪ Track infections from email 	<ul style="list-style-type: none"> ▪ Unified threat management ▪ Endpoint security solution that includes botnet, virus, and Trojan protection ▪ Outbound filtering to ensure email is malware free ▪ Anti-spoofing, anti-phishing, anti-spyware, anti-keylogger, anti-fraud solutions ▪ Monitoring outbound traffic for botnet activity ▪ Attachment filtering ▪ Automated email policy enforcement ▪ Quarantine questionable inbound email ▪ Real time monitoring of outbound email for sensitive data ▪ Alerting email users to inappropriate outbound email use ▪ Intervention of inappropriate outbound email ▪ Integrated email and web security ▪ Visibility into threats across desktops, servers, networks

Source: Aberdeen Group, August 2008

Best-in-Class Strategies

Across all classes, the top three strategies employed focus first on inbound vulnerabilities, next on outbound vulnerabilities, and third on training users in appropriate email usage.

Figure 2: Best-in-Class Strategies for Email Security



Source: Aberdeen Group, August 2008

“With the proliferation of mobile devices with email capabilities, some control is taken out of our hands as to the data security.”

~ Manager of Information Technology of a \$300M Financial Services Company

Aberdeen Insights — Strategy

Policy at the core

Email security relies on the existence and enforcement of policies that apply to every dimension of email. Inbound email policies determine what mail is allowed in and include all the rules that are invoked to prevent spam.

Inbound policies are part of every anti-spam solution and can be applied in the cloud, at the perimeter of an organization's network as well as on the email user's endpoint device(s). Inbound policies might relegate questionable email to quarantine or reject email from domains that have been blacklisted.

Outbound policies can include rules for monitoring outbound email for spam and malware infection as well as for the transmission of sensitive data. Outbound policies might also specify blocking the sending of sensitive data, encrypting sensitive data on the fly, or notifying users or administrators of inappropriate data use.

Data use policies should apply to data in transmission within an organization as well as data included in outbound messages.

continued

Aberdeen Insights — Strategy

Organizations should articulate the legitimate use of email in acceptable use policies and use automated solutions to enforce these policies wherever possible. Training users in appropriate email use is paramount. Automated solutions can go a long way to curb inadvertent misuse by users that are unaware of data use policies, and help train users by notifying them of unacceptable use.

Best-in-Class organizations use role-based email policies that specify appropriate email usage by the role of the user.

Inbound email protection

Experts agree that at least 80% and perhaps as much as 99% of all email that is generated is spam - unwanted, unsolicited, and, more often, pernicious email sent with the express purpose of perpetrating crime. With estimates of some 130 billion messages created daily, of which at least 100 billion are spam, it's no wonder that organizations put protecting themselves against inbound email as their first priority.

A significant source of malicious spam comes from organized criminal elements that fund the ongoing development of threats. New email threats perpetually emerge, and this year 31% of organizations report an increase in malicious mail targeted to specific individuals. An increasing number of threats rely on targeted phishing, social engineering or leveraging known behaviors of the targeted individuals.

Outbound email protection

Preventing data loss - intentional or accidental - requires the ability to monitor outbound email for sensitive data, well-defined data use policies, and protecting email in transit. In addition, organizations must protect against infected machines under their purview disseminating spam or infected email. Beyond the deliberate sharing of sensitive data and data lost inadvertently through such accidents as selecting the wrong auto-filled address, spyware, and key loggers - often deployed by sites that users were directed to by email - divulge sensitive data from a users' computer and from capturing users' key strokes.

Protecting data at home and abroad

Sensitive data requires special handling within an organization and outside of the organization. If sensitive data can be emailed within an organization or copied without limit (that is, if protection is placed only on outbound email), the sensitive data is not adequately protected.

In the next chapter, we see what the top performers do to protect their email.

Chapter Two: Benchmarking Requirements for Success

Creating a comprehensive email security strategy involves determining appropriate processes, allocating the necessary organizational support and selecting the technology solutions best suited to ensure secure email in a particular environment.

Case Study - Minimizing Risk in a Highly Regulated Environment

The Vice President in charge of Internet and Email Security for a leading financial services firm shared the challenges of email security for any organization in a regulated industry. Because email is intricately involved in business process, looking at the flow of email internally and externally reveals many levels of complexity.

As a company doing business in a regulated industry, they are mandated by legislation to keep records showing the flow of information and must be able to show control over the message flow. "It's time consuming and expensive – coordinating and tagging accounts, not dropping things in the flow, ensuring that there are no alternate routes that would make the records incomplete. It's heavy weight programming, dedicated journaling, and archiving," said the Vice President, Internet and Email Security. "People often underestimate the level of integration necessary to really ensure email security. The number of dependencies into and out of our email structure is not immediately evident – you have to pull on a string and see what happens. You can't just say 'Let's move this server.' What about the integration with Active Directory? What about the Certificate Authority? Asking 'What are all the business processes that got us to this point?' has been very effective for us."

The need to drive costs down led this company to outsource email management. For this they had to extend their data loss prevention strategy to include the outsourced services and negotiate appropriate service level agreements appropriate for each of their customers. Their routing rules had to be extended to include the service provider. "On our own systems, once we send something, we consider it delivered. We had to establish what that means in an outsourced environment. Different ISPs handle things differently so we have to be careful to make sure we understand what happens in each environment. Some email gets routed over a VPN or dedicated circuit, some goes through a hybrid solution or is outsourced – we always have to do the traffic analysis to see what's not standard," said the Vice President, Internet and Email Security.

continued

Fast Facts

- √ 81% of Best-in-Class organizations scan outbound messages for spam and malware verses 63% of all organizations
- √ Best-in-Class organizations verify email senders' authenticity two and a half times more than Laggard organizations

Case Study - Minimizing Risk in a Highly Regulated Environment

As a financial institution they are susceptible to phishing attacks on a wide scale. They have to be attentive to any activity that is associated with any of their domains. When attacks surface in their name, they need to be active to knowing where they're coming from and shutting them down quickly. For them, their email security strategy involves a wide spectrum of solutions carefully deployed to ensure security and regulatory compliance. For any organization in a regulated industry the advice is: "If you're not thinking this way - shame on you - you need to be."

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 their results to improve their 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
Process	Role-based email policy		
	46%	34%	32%
	Email acceptable use policy		
	81%	81%	75%
	Manual enforcement of acceptable use policy		
	58%	54%	45%
Organization	User training in safe email practices		
	77%	54%	50%
	Individual responsible for reviewing email abuse reports		
	64%	40%	35%
	Individual responsible for reviewing inbound mail in quarantine		
	73%	53%	45%

	Best-in-Class	Average	Laggards
Knowledge	Real-time end-user notification of inappropriate email use		
	58%	28%	26%
	Data use reports		
	65%	40%	30%
	Email use report		
	67%	53%	41%
	Visibility into threats across desktops, servers and networks		
	58%	49%	45%
Performance	Email threat reports		
	77%	51%	46%
	Track fraud from email		
	37%	23%	21%
	Track infections from email		
	69%	47%	40%
Technology Enablers	Inbound email protection		
	100%	96%	87%
	Verification of email sender's authenticity		
	64%	49%	25%
	Protection for email in transmission		
	65%	52%	26%
	Ensure outbound messages are malware free		
	74%	61%	45%
	Monitor outbound traffic for botnet activity		
	60%	34%	23%
	Scan email attachments for sensitive data		
	65%	35%	31%
	Integration of email security with web security		
	74%	45%	23%
	Identify and respond to new threats in a timely and automated manner		
	85%	56%	57%
	Protection of web mail		
	62%	49%	29%
	Protection of other email enabled resources		
	52%	38%	16%
Automated enforcement of acceptable use policy			
27%	24%	17%	
Endpoint security that includes botnet, virus and Trojan detection			
77%	67%	42%	
Anti-spoofing, anti-phishing, anti-spyware, anti-key logger, anti-fraud solutions			
78%	68%	47%	

	Best-in-Class	Average	Laggards
Technology Enablers (cont.)	Quarantine questionable inbound email		
	42%	35%	21%
	Real time monitoring of outbound email for sensitive data		
	42%	25%	17%
	Intervention of inappropriate email		
	42%	36%	23%

Source: Aberdeen Group, August 2008

Capabilities and Enablers

Based on the findings of the Competitive Framework and interviews with end users, Aberdeen’s analysis of the Best-in-Class demonstrates that using an email security strategy that leverages policy, organizational support, usage and performance data, as well as a spectrum of technology enablers can result in reducing data loss, infections from email, lost productivity and costs associated with remediation required as the result of successful email attacks.

"I was victimized by a very clever attack. Because I very much care about my customers, I felt compelled to open something that looked like a customer complaint."

~ CEO of a Software Company

Process

Policy, policy, policy. The key to secure email strategies is the creation and enforcement of appropriate strategies from end to end. Policies need to be consistent and consistently enforced, and organizations need to establish processes to review and extend or refresh policies regularly. Because protecting data involves limiting access to data to those with legitimate access, organizations need to establish roles that include access rights. Extending these roles to email policies is movement in the direction of coherent, consistent policies that can be uniformly enforced.

Organization

User training in safe email practices is key in curbing data loss from email as well as preventing successful phishing, scams, and social engineer attacks.

Users need to clearly understand what can and cannot be sent through email, or what can be sent to whom and under what conditions. Despite evidence that most users have heard the idea that email sent "in the clear" - that is, unprotected, unencrypted - too many believe that no one is interested in their particular mail, so sending data through email is safe for them. Most are unaware that automated software is scanning email looking for certain kinds of information, and that there is an active market for this kind of data. Organizations must also ensure that users understand that proprietary information including the organization's intellectual property, financial information, and personnel data are highly sensitive information and should never be sent unprotected and only sent in compliance with specific organizational guidelines.

Users need to be taught to recognize tell-tale signs of phishing attacks and how to look out for scams and clever ruses. Increasingly, specific individuals are being targeted (sometimes known as spear-phishing) with personalized attacks aimed at getting them to inadvertently divulge sensitive

data or be lured to a malicious site that may infect their computer with malware which in turn can be used to get at personal data.

Organizations need to designate people responsible for reviewing email abuse reports as well as inbound mail in quarantine. Without attention to these reports, organizations may be missing valuable information key to their security strategies.

Knowledge Management

Some inappropriate use of email is unintentional, some is not. Often the simple act of notifying users of inappropriate use acts as a training device and deterrent to misuse. Organizations need data use and email use reports to develop appropriate policies and detect aberrant behaviors.

Because more threats leverage multiple channels, visibility into threats across servers, desktops and networks can lead to earlier detection and remediation.

Technology

Protecting Organizations from Inbound Email Threats

All Best-in-Class organizations have explicit protection for inbound threats. What's surprising is that not every organization does. Anti-spam solutions use various means to sort spam from legitimate mail including verifying the email senders' authenticity, relying on the reputation of the sender's domain, and detecting activity across addresses and networks. To prevent important email from being potentially lost in a spam filter, Best-in-Class organizations often use solutions that put questionable mail into quarantine to await further evaluation.

Not protecting against inbound threats not only puts the organization itself at risk but also makes the organization's assets more susceptible to exploitation. For example, the organization's computers may be infected with botnets and may be unwittingly distributing spam or participating in cyber attacks.

The window of vulnerability to attack from a new threat lies in the time between the new threat being launched and the new threat being detected and appropriate protection against it created and disseminated. An organization's **unnecessary** window of vulnerability lies in the time between protection becoming available and protection being deployed. With new threats being created constantly, waiting hours, let alone days, to protect against a new threat is tantamount to going without sunscreen in the tropics - eventually you're going to get burned.

More inbound email threats use innocuous looking email to entice users to malicious sites that subsequently infect their computer or dupe them into divulging sensitive data. To thwart these kinds of ploys, Best-in-Class organizations integrate the email and web security and deploy solutions targeted to foil spoofing, phishing, spyware, key loggers, and fraud.

Protecting the Organization against Outbound Email Vulnerabilities

Aberdeen research indicates that email is considered one of the most serious channels for data loss - either intended or accidental. Best-in-Class organizations use several different kinds of solutions to prevent or intercept potential data loss events. They use automation to enforce acceptable use policies; they monitor outbound email for sensitive data; they scan email attachments for sensitive data; and they detect inappropriate email use and take specific actions to notify the sender (or others) or block the email.

Further, Best-in-Class companies protect email in transmission. Email encryption that does not place a burden on the email users (both sender and receiver) should become best practice for every institution.

Outbound spam or infected email can cause damage that the organization may be held accountable for and, at a minimum, can cause serious damage to the organization's brand. Phishing attacks that go unchecked by the organization whose identity is being spoofed can create serious brand damage in ill-will. Organizations need to ensure that their outbound messages are spam and malware free and need to monitor their outbound traffic for botnet activity.

Bolstering Email Protection

Best-in-Class organizations use endpoint security that includes botnet, virus and Trojan detection, and they explicitly protect web mail and other email enabled resources such as wikis.

Performance Management

Without tracking email security incidents such as data loss, infections and fraud, organizations have a difficult time demonstrating the effectiveness (or lack thereof) of their email security strategy. Monitoring performance on an ongoing basis is critical to keeping up security despite ever-more pernicious attacks.

Aberdeen Insights — Technology

Email is mission critical to every organization. Because the risks associated with email vulnerabilities are great and because the insurmountable volume of ever-more sophisticated attacks constantly increases, email is a technology that needs extensive technology and strategy to protect the organization from the vulnerabilities that are inherent in its use.

Ultimately, larger organizations will need an extensible email or messaging architecture to ensure comprehensive email security. This architecture must support the creation and enforcement of policies and allow the easy incorporation of new email security solutions as they arise. Neither the email threat landscape nor regulatory initiatives are static - each continue to evolve and will continually require new approaches to protect, inspect, and enforce compliance with both internal security policies and external regulations.

Chapter Three: Required Actions

Whether a company is trying to move its performance in mail security from Laggard to Industry Average, or Industry Average to Best-in-Class, the following actions will help spur necessary performance improvements:

Laggard Steps to Success

- Respond immediately and automatically to new threats. Only 47% of Laggard organizations respond immediately and automatically to new threats, compared with 85% of the Best-in-Class. Thirty percent (30%) of Laggard organizations wait at least a day for updates - some as much as a week. No Best-in-Class company waited more than eight hours.
- Protect email in transmission. Best-in-Class organizations protect email in transmission two and a half times more often than Laggard organizations. Because email encryption can now be done transparently, the excuse of its being too cumbersome for the end-user no longer holds.
- Use best-of-breed solutions and a layered approach to stopping spam. Eighty-nine percent (89%) of Laggard organizations report an increase in SPAM reaching users' inboxes, compared with 34% of Best-in-Class companies. Laggard organizations need to look at significantly better anti-spam strategies that can deliver much better results.
- Use best-of-breed solutions directly targeting spyware and key loggers. Fifty percent (50%) of Laggard companies report an increase in spyware and key logging events compared with only 16% of the Best-in-Class. Laggard organizations need better anti-spyware, anti-key logging strategies.
- Monitor outbound mail for botnet activity. Compared to the Best-in-Class (60%), only 23% of Laggard organizations monitor their outbound mail for botnet activity. Botnet infections are perhaps the most difficult malware to detect. Botnets hide very effectively and change frequently. Their intent is not to harm the machine they're on, rather to co-opt it for use in short attacks and then go back into hiding to attack again another day. Without specifically looking for botnet activity (which is changing all the time), it's no wonder that the estimated hundreds of millions of infected machines mostly remain undetected. As botnets are the primary distributors of spam, when botnets are activated, the results can be disastrous for the organization whose computers have been enlisted in the attack. Organizations may find their systems shutting down without their knowing the cause or how to stop it from happening again.

Fast Facts

- √ Laggard companies are more than twice as likely as Best-in-Class companies to complain about SPAM on a daily basis
- √ 41% of the Best-in-Class companies believe that, after email, the messaging channel that poses the biggest threat is instant messaging

"This is a continuous struggle with ever-changing technology in the wrong hands."

~ Business Process Consultant to a Municipal Government with more than 2500 email users

Industry Average Steps to Success

- Monitor outbound mail for spam and malware. Compared with the Best-in-Class (81%), only 57% of Industry Average organizations monitor outbound mail for malware and spam. Sending out infected mail can cause further contamination within an organization and create ill-will and damage for partners, customers and prospects – any entity with which they exchange email. Organizations whose email addresses have been harvested by spammers or whose computers are part of a botnet – the virtual spamming infrastructure – may soon find that their domain has been blacklisted and that they have difficulty sending legitimate mail. An organizations domain's reputation is directly connected to their brand and must be protected.
- Protect email in transmission. Compared with the Best-in-Class (65%), only 52% of Industry Average organizations protect email in transmission. Because email encryption can now be done transparently, the excuse of its being too cumbersome for the end-user no longer holds.
- Integrate email and web security. Sixty-seven percent (67%) of the Best-in-Class already have integrated email and web security, compared to 47% of the Industry Average. More threats are “blended” attacks that use a combination of seemingly innocuous email (not caught by anti-spam, anti-phishing, anti-malware solutions) to entice users to a malicious site that can infect their machine and potentially compromise sensitive data. Integrating email and web security helps organizations detect and protect against these kinds of attacks more quickly.
- Monitor outbound mail for botnet activity. Compared to the Best-in-Class (60%), only 34% of Industry Average organizations monitor their outbound mail for botnet activity. Botnet infections are perhaps the most difficult malware to detect. Botnets hide very effectively and change frequently. Their intent is not to harm the machine they're on, rather to co-opt it for use in short attacks and then go back into hiding to attack again another day. Without specifically looking for botnet activity (which is changing all the time), it's no wonder that the estimated hundreds of millions of infected machines mostly remain undetected. As botnets are the primary distributors of spam, when botnets are activated, the results can be disastrous for the organization whose computers have been enlisted in the attack. Organizations may find their systems shutting down without their knowing the cause or how to stop it from happening again.

Best-in-Class Steps to Success

- To prevent sensitive data from leaving an organization, organizations need to determine what constitutes sensitive data, who has legitimate access to what data, and under what conditions can that data be sent through email (and to whom). All this requires email policies that can intervene in the dissemination of sensitive data through email. Notifying users in real time about inappropriate email use can minimize both intentional and accidental data loss through email. Although Best-in-Class companies already do this to a much greater extent than other organizations - 58% verses Industry Average (28%) and Laggard (26%), there's still a lot of room for improvement.
- Beyond simply notifying users, organizations should take specific actions when users send email that violates acceptable usage policies, including data use policies. Using automated solutions that block, encrypt, return, or take other specific actions help protect the organization and its data. Although well ahead of Industry Average companies (36%) and Laggard companies (23%), only 42% of the Best-in-Class companies intervene in the sending of inappropriate email.
- To effectively and consistently protect data inside email requires that the organization define user roles and access appropriate to these roles. Once created, these roles can be used to enforce email policies on a more granular level. Although well ahead of the Industry Average and Laggard classes, only 46% of the Best-in-Class currently use role-based email policies. Role definitions and policies that leverage them can help organizations gain better control over their email flow and meet regulatory compliance.
- Email vulnerabilities exist in all messaging resources and organizations must protect web mail, IM, wikis, blogs and other email enabled resources. Although well ahead of the Industry Average and Laggard classes, only 62% of the Best-in-Class currently protect web mail, and only 52% currently protect other email-enabled resources. Using web mail to access mail can leave organizations vulnerable in ways they make think themselves otherwise protected.

Aberdeen Insights — Summary

Email - and email vulnerabilities - are here to stay. Organizations are well-advised to create and enforce extensible, flexible email security policies and strategies that address inbound email vulnerabilities, the vulnerabilities associated with outbound threats, and the use of email within the organization.

continued

Aberdeen Insights — Summary

Email security is integrally connected with the security of an organization's data, infrastructure, and brand. An email security strategy needs to be cognizant of and interface well with both data security and infrastructure security.

Because email threats perpetually evolve, organizations must be vigilant in keeping current with what's necessary to keep the organization and its assets safe. Inadequate email protection puts an organization at risk. Yet the myriad vulnerabilities that email enables provide a management challenge to those responsible for email security, and over time, organizations are changing to try to gain better control. Further, because the volume of email (legitimate and not) continues to grow exponentially, organizations need platforms that will scale exponentially.

Seventy-five percent (75%) of Best-in-Class organizations changed their email strategy in the last two years - 30% in the last six months. The number one reason for change? Such companies believe they can get better control and management.

Send to a Friend 

Appendix A: Research Methodology

Between June and July 2008, Aberdeen examined the use, the experiences, and the intentions of more than 170 enterprises using email security in a diverse set of enterprises.

Aberdeen supplemented this online survey effort with 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: C-level executive (32%), VP / Director (20%); Manager (21%); and Consultant / Staff (23%).
- *Industry:* The research sample included respondents from a cross section of industries such as: high technology / software (32%), finance / accounting / banking (16%); computer equipment and peripherals (10%).
- *Geography:* The majority of respondents (61%) were from North America. Remaining respondents were from the Asia-Pacific region (15%) and Europe (22%).
- *Company size:* Twenty-three percent (23%) of respondents were from large enterprises (annual revenues above US \$1 billion); 25% were from midsize enterprises (annual revenues between \$50 million and \$1 billion); and 52% of respondents were from small businesses (annual revenues of \$50 million or less).
- *Headcount:* Forty-three percent (43%) of respondents were from small business (headcount between 1 and 100 employees); 21% were from midsize enterprises (headcount between 100 and 999 employees); and 37% of respondents were from large enterprises (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

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

- √ The degree to which email security is deployed in their operations
- √ 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 4: 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>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)</p> <p>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)</p> <p>Capabilities — the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products / services, ecosystem partners, financing)</p> <p>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)</p>

Source: Aberdeen Group, August 2008

Table 5: 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>Best-in-Class (20%) — 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>Industry Average (50%) — Practices that represent the average or norm, and result in average industry performance.</p> <p>Laggards (30%) — Practices that are significantly behind the average of the industry, and result in below average performance.</p>	<p>In the following categories:</p> <p>Process — What is the scope of process standardization? What is the efficiency and effectiveness of this process?</p> <p>Organization — How is your company currently organized to manage and optimize this particular process?</p> <p>Knowledge — What visibility do you have into key data and intelligence required to manage this process?</p> <p>Technology — What level of automation have you used to support this process? How is this automation integrated and aligned?</p> <p>Performance — What do you measure? How frequently? What’s your actual performance?</p>

Source: Aberdeen Group, August 2008

Table 6: 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, August 2008

Appendix B: Related Aberdeen Research

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

- [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](#)
- [Data Loss Prevention: Little Leaks Sink the Ship June 2008](#)

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

Author: Carol Baroudi, Sr. Research Analyst, Security,
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.

043008a