

## **Secure / Managed File Transfer**

Why Best-in-Class Companies are saying it's a "Must Have"

September 2008

Carol Baroudi

## Executive Summary

The demand for easy to use, secure file transfer has grown from quiet rumblings to loud demands as organizations face pressures on many fronts. Data privacy legislation requires sensitive data be protected both at rest and in motion. Gigantic files containing media content, check images, health care records, design graphics, weather data, and more are the currency of everyday business but their size throttles email systems and creates a heavy demand on the storage necessary to support email archives. Legacy file transfer solutions are proving insecure, too cumbersome or too expensive. Distributed work forces require easy, safe file transfer on demand. Ad hoc collaboration within an organization and with customers, partners, and suppliers facilitates business process while creating a security nightmare. Cloud collaboration is overshadowed by a dearth of secure file transfer. Green initiatives point to the use of physical media and costly, fuel-guzzling courier services as good targets for replacement by electronic file transfer.

### Best-in-Class Performance

Aberdeen used four key performance criteria to distinguish Best-in-Class companies' use of file transfer:

- Number of actual data loss incidents
- Number of data loss incidents attributable to file transfer
- Total cost of addressing data loss incidents
- Average time to address data loss incidents from file transfer

### Competitive Maturity Assessment

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

- 45% reduced non-compliance incidents related to data protection
- 45% reduced the cost of responding to non-compliance issues related to data protection
- 30% reduced help desk calls associated with file transfer

### Required Actions

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

- Get a comprehensive understanding of the needs for file transfer across their organization
- Ensure that all file transfers comply with internal security policies and external regulation
- Train users in file transfer policy and best practices

#### 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 as a security conscious organization, invest in what is necessary, adequate, and sufficient after due diligence to protect our information assets. Secure file transfer is definitely one critical area and we are constantly educating users, have already put in place policy and control mechanisms. We are also evaluating various tools for automated monitoring and alerting."

~ Information Security Management

\$14B Financial Services Organization

## 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
The Demand for Secure / Managed File Transfer.....	4
Eschewing FTP.....	4
Why Email is Not a Good Substitute for Secure File Transfer.....	5
Green Data Transport.....	6
Secure / Managed File Transfer.....	6
The Maturity Class Framework.....	7
The Best-in-Class PACE Model.....	8
Best-in-Class Strategies.....	10
Chapter Two: Benchmarking Requirements for Success.....	12
Competitive Assessment.....	12
Capabilities and Enablers.....	14
Chapter Three: Required Actions.....	17
Laggard Steps to Success.....	17
Industry Average Steps to Success.....	17
Best-in-Class Steps to Success.....	18
Appendix A: Research Methodology.....	19
Appendix B: Related Aberdeen Research.....	21

## Figures

---

Figure 1: Drivers Demanding Secure File Transfer.....	7
Figure 2: Top Strategies Driving Investment in Secure / Managed File Transfer Solutions.....	11

## Tables

---

Table 1: Top Performers Earn Best-in-Class Status.....	8
Table 2: The Best-in-Class PACE Framework.....	10
Table 3: The Competitive Framework.....	13
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

### The Demand for Secure / Managed File Transfer

---

The convergence of a spectrum of factors is compelling most organizations to formalize or re-think their strategies around file transfer. File transfer - the movement of a file from point A to point B directly - specifically not as an attachment to email - is not new. Major corporations across industries have been doing this for decades; auto manufacturers transfer parts inventories, banks transfer transaction records, and retailers transfer pricing information and inventory, for example. Some enterprises transfer literally hundreds of thousands of files every day.

What is new are the pressures from various sources that are calling for file transfer capabilities to be widely available across the organization, easy to use, safe (from a data protection and regulatory compliance perspective), reliable, auditable, scalable, with guaranteed delivery - just for starters. New too are the huge files associated with the explosion of rich content - not just audio and video and design graphics, but also images of checks that banks are using to reduce the costs associated with handling paper checks. And the demand for file transfers in support of ad hoc collaboration with business partners, suppliers, and customers is different from the orchestrated file transfers common to the enterprise.

To meet these demands a wide pool of vendors are offering a variety of file transfer solutions. Because organizations vary widely in what they use file transfer for, there is no "one size fits all" solution. What is clear is that the demand for these solutions is heating up, and, as file transfer always involves both a sender and receiver, the current demand is likely to spark still more growth.

### Eschewing FTP

---

The File Transfer Protocol (FTP) is a network protocol that was first defined in 1971, 20 years before the Internet was in the public domain, nearly a half century ago. The protocol has been updated and is now often run over networks which themselves have been secured, but it was never designed for the widespread use required of file transfer solutions today, and never had security as a prime objective.

Because FTP is widely available for free, it's found its way into organizations of every size and is often embedded in scripts which themselves may be obsolete. Somewhat akin to the orphaned accounts left by users who were never de-provisioned, thousands of file transfers continue to happen daily in legacy environments that have simply lost track.

The problems with using FTP in today's business environment are myriad. The following are some of them:

#### Fast Facts

- √ 83% of Best-in-Class companies use a secure file transfer solution
- √ 76% of Best-in-Class companies use managed file services versus only 23% of Industry Laggards
- √ 25% of Best-in-Class companies reduced data loss incidents related to email attachments versus 0% of Industry Average and Laggard companies

- Plain FTP has no inherent method for encryption - data is sent in the clear and therefore "sniffable" by eavesdroppers
- Requests to enable a new FTP account often puts extra demand on system administrators and sometimes takes days for the request to be fulfilled - an unacceptable delay for time sensitive transfers
- FTP is a manual process and files placed on an FTP server stay there until manually deleted
- FTP servers themselves are often not secure enabling users access to data not intended for them
- FTP has no mechanisms to verify if a transfer is complete and the receiver has no mechanism to determine the integrity of the file received.

Organizations need to root out all unsecured FTP usage and define and enforce policy precluding the use of unsecured FTP. Because FTP is easily obtained for free for almost all platforms, if organizations fail to provide adequate file transfer support and enforce file transfer policy, knowledgeable users will continue to circumvent delays in requests for support and take advantage of this unsecured channel.

## Why Email is Not a Good Substitute for Secure File Transfer

Many organizations are finding their way to using secure file transfer solutions because doing business now entails the electronic exchange of large files in ways that have not previously been envisioned. With the explosion of rich, digital content - graphics, video, audio, even PowerPoint presentations - organizations find that email is often not the right choice for getting files from point A to point B. Email gateways are often configured to restrict attachment sizes, typically to 10 megabytes. Though the gateways can be reconfigured, to allow larger attachments, email was not designed to handle extremely large files and their delivery often proves problematic. Further, with organizations moving toward email archiving - in some places it's already mandated - storing large attachments (and some times multiple copies of large attachments) begins to take a toll on storage requirements. In many organizations the amount of email storage allowed has an explicit cap, and a few large file attachments can fill an email storage quota quickly.

Even small attachments of only one meg, for example, can be cumbersome if sent across a company of 1,000 employees. Best practices suggest that the file be put on a secure server with a link in the email, obviating the need to archive 1,000 copies. This solution addresses the excessive storage demands but begs the question of e-discovery. If external or internal policies require that email be archived for any length of time, how will the link embedded in the email en lieu of the attachment resolve in a year or two or six?

Recent Aberdeen research found that 67% of Best-in-Class companies give special attention to handling large attachments. Some secure file transfer vendors provide a seamless user interface in the email client so that, either

### Fast Facts

- √ 35% of Best-in-Class organizations were able to reduce human error related to file transfers verses 13% of Industry Average organizations and 3% of Laggards
- √ 83% of Best-in-Class companies control their network ports as part of their secure file transfer strategy verses only 63% of Industry Average and 53% of Laggard organizations

by intention or by policy, large attachments are stripped off the email message, moved to a server, and a secure link is provided in the email. When recipients receive the email, they click on the embedded link to download the attachment.

## **Green Data Transport**

---

Despite the availability of high-speed networks many organizations have persisted in creating and transporting physical media such as CDs, DVDs, and even magnetic tapes. The physical media is then shipped to the receiver(s) often incurring premium shipping costs for expedited delivery. More organizations are recognizing that they can send the bits without the cost of creating the physical media and without the rising costs of physical delivery. What's more, the direct file transfer is faster.

Even contracts that are frequently sent overnight for signature can be replaced with digital documents coupled with an electronic signature. Organizations transferring files across international borders are avoiding the delays at customs often associated with physical media entering the country. Businesses are enjoined to "stop shipping and start saving."

## **Secure / Managed File Transfer**

---

Recognizing the inherent shortcomings of FTP, many organizations sought safety in SSH-File Transfer Protocol (SFTP) only to find that it wasn't the panacea they sought. SFTP is very platform-dependent, not native to Windows, and not welcome on many systems. Nor does it solve the need for an easy to use file transfer mechanism appropriate for business users.

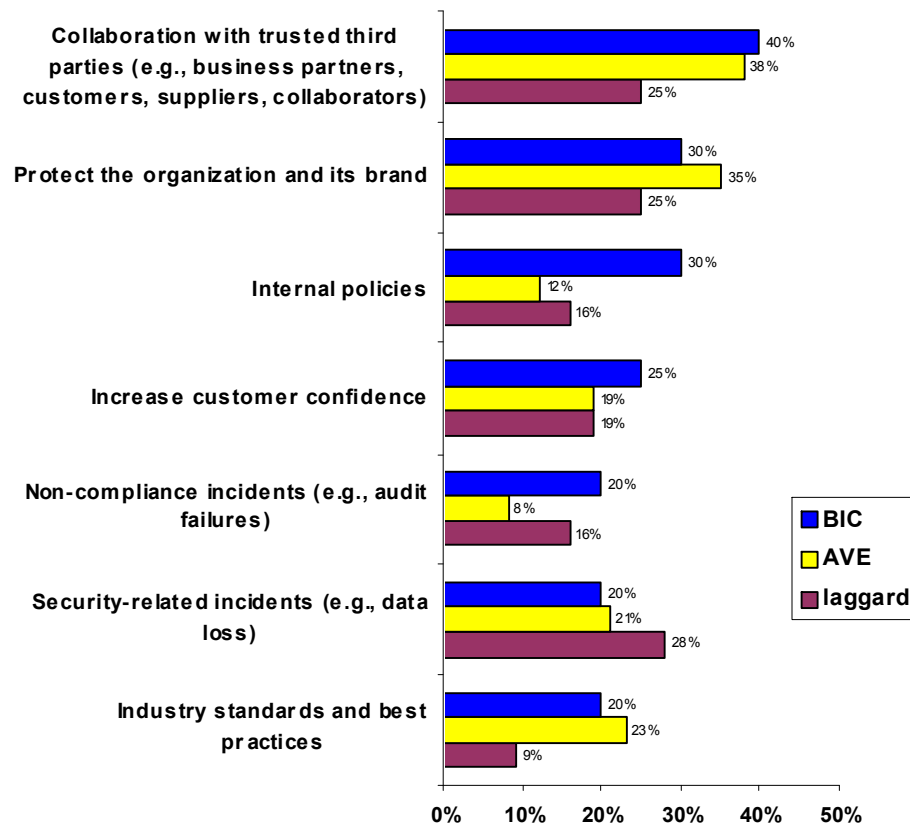
Organizations that recognize file transfer as integral to their business processes understand that file transfer is not an end in itself - it is the transport mechanism for moving data from one process to the next in a work flow. To ensure that the data moves smoothly and securely and that it arrives in tact at its target destination (and no where else), organizations often need to integrate with both key internal applications and the key applications used by their partners / collaborators / suppliers / customers. They need to ensure that critical files are received in tact, and, if a transmission fails for any reason, it needs to pick up where it left off, or start again, or notify someone who can correct whatever's wrong.

All the nuance of that goes beyond the mere transport of the data can be seen as the management of the file transfer. For all these reasons, managed file transfer is what most organizations really need. Secure file transfer is now table stakes. The focus now is on how much control, flexibility and power organizations stand to gain.

Beyond ensuring the in-tact delivery of data to the intended party, organizations can now accelerate file transfers or control bandwidth to increase and decrease speed. When transfers that traditionally take hours can be reduced to minutes, even more applications that can take advantage

of higher speeds of delivery will provide strategic advantage and still more data will flow.

**Figure I: Drivers Demanding Secure File Transfer**



Source: Aberdeen Group, September 2008

The number one driver for organization's focus on secure / managed file transfer is collaboration with trusted third parties. As organizations expand their relationships the need to transfer more and bigger files faster is likely explode. As one person explained it, "Don't underestimate the title wave effect." Her organization anticipates their volume doubling year over year - from what began as 200GB of transferred data, to 400, to 800, and beyond.

**The Maturity Class Framework**

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

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

Definition of Maturity Class	Mean Class Performance
<p><b>Best-in-Class:</b> Top 20% of aggregate performance scorers</p>	<ul style="list-style-type: none"> <li>▪ 45% decreased the total number of data loss incidents</li> <li>▪ 45% decreased the number of data loss incidents attributable to file transfer</li> <li>▪ 40% decreased the total cost of addressing data loss incidents</li> <li>▪ 50% decreased the average time to address data loss incidents from file transfer</li> </ul>
<p><b>Industry Average:</b> Middle 50% of aggregate performance scorers</p>	<ul style="list-style-type: none"> <li>▪ 9% decreased the total number of data loss incidents</li> <li>▪ 4% reduced of data loss incidents attributable to file transfer</li> <li>▪ 2% decreased the total cost of addressing data loss incidents</li> <li>▪ 6% reduced the average time to address data loss incidents from file transfer</li> </ul>
<p><b>Laggard:</b> Bottom 30% of aggregate performance scorers</p>	<ul style="list-style-type: none"> <li>▪ 0% decreased the total number of data loss incidents</li> <li>▪ 0% decreased the number of data loss incidents attributable to file transfer</li> <li>▪ 3% reduced the total cost of addressing data loss incidents</li> <li>▪ 0% decreased the average time to address data loss incidents from file transfer</li> </ul>

Source: Aberdeen Group, September 2008

### The Best-in-Class PACE Model

Securely transferring files requires a combination of strategic actions, organizational capabilities, and enabling technologies. Organizations often categorize their file transfer needs in two ways:

- Regularly scheduled file transfers such as daily transaction records sent from distributed locations to a centralized hub or backups of log files
- Ad hoc file transfers such as sending a large file to a partner or collaborator

Alternatively, some organizations categorize their file transfer needs somewhat differently:

- Business to business file transfer or machine to machine file transfer or perhaps, more accurately, process to process file transfer, where the file transfer is initiated by one process and received by another automatically, without direct human initiation

- Human to human file transfer where the individual sender transfers the file to a specific individual

Neither of these categorizations is really satisfying. The types of file transfer needs are not so easily defined. Some organizations regularly schedule file transfers between individuals. The categories are the industry's attempt to cordon off areas of functionality in order to align certain problems with existing solutions which have emerged from the specific kinds of problems they were initially created to address.

Concerns about data protection apply to all types of file transfer. File transfers are an integral part of business process, whether or not they are explicitly defined in an organization's work flow. And file transfers of every type are on the rise across organizations of every kind. Of the organizations we surveyed:

- 63% reported an increase in the volume of outbound file transfers
- 60% reported an increase in the volume of inbound file transfers
- 49% reported an increase in ad hoc file transfers
- 47% reported an increase in file transfers within their organizations

Simultaneously, access to sensitive data is on the rise. Of the organizations we surveyed:

- 37% reported an increase in the number of employees with access to sensitive data
- 30% reported an increase in the number of contractors with access to sensitive data
- 31% reported an increase in the number of business partners with access to sensitive data
- 32% reported an increase in the number of customers with access to sensitive data

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

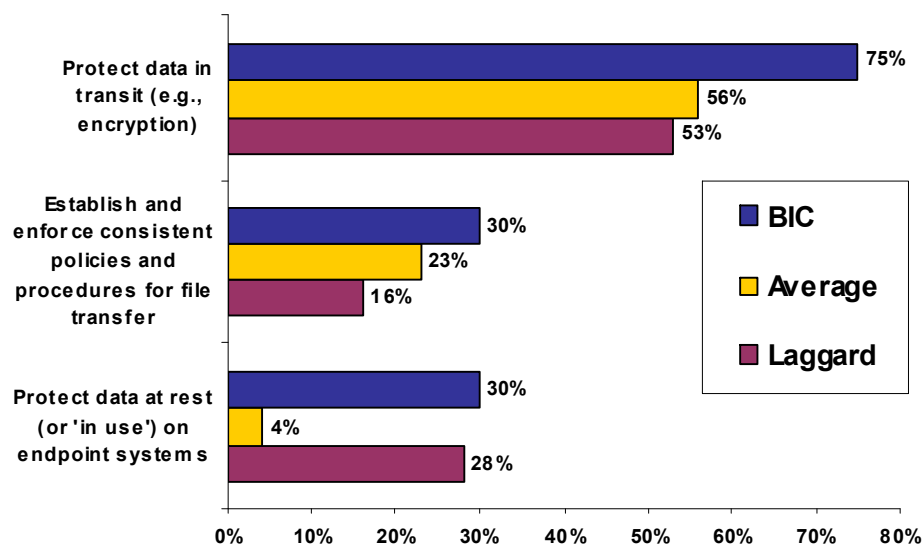
Pressures	Actions	Capabilities	Enablers
<ul style="list-style-type: none"> <li>▪ Collaboration with trusted third parties such as business partners, customers, suppliers and collaborators</li> </ul>	<ul style="list-style-type: none"> <li>▪ Protect data in motion</li> <li>▪ Protect data at rest</li> <li>▪ Establish and enforce consistent policies and procedures for file transfer</li> </ul>	<ul style="list-style-type: none"> <li>▪ Consistent policies for sending files</li> <li>▪ Consistent policies for receiving files</li> <li>▪ Consistent policies for data at rest</li> <li>▪ Reporting of all file transfer activity</li> <li>▪ Real-time notification of policy violations</li> <li>▪ Responsible executive or team with primary ownership for data protection</li> <li>▪ Information classified by requirements for confidentiality, integrity and availability</li> <li>▪ Risk assessment</li> <li>▪ Identified source (channel) of data loss incidents</li> </ul>	<ul style="list-style-type: none"> <li>▪ Secure File Transfer solution</li> <li>▪ Managed file transfer service</li> <li>▪ Multi-tiered network architecture</li> <li>▪ Integration of file transfer system with AD, LDAP, ODBC or other access control database</li> <li>▪ Integration of File Transfer solution with key internal applications</li> <li>▪ Integration File Transfer solution with key applications of trusted partners (customers, collaborators, partners, suppliers)</li> <li>▪ Checkpoint restart - Automatically restarts at point of failure</li> <li>▪ Automatic retry after transmission failure</li> <li>▪ Guaranteed file delivery</li> <li>▪ Authentication of file recipient</li> </ul>

Source: Aberdeen Group, September 2008

### Best-in-Class Strategies

Protecting the data in transit is the leading strategy being employed by Best-in-Class organizations investing in secure / managed file transfer solutions. Next is establishing and enforcing policies around file transfer which is critical to long-term success in protecting data and establishing and maintaining compliance. Keeping data safe at rest is also integral to these goals.

**Figure 2: Top Strategies Driving Investment in Secure / Managed File Transfer Solutions**



Source: Aberdeen Group, September 2008

**Aberdeen Insights — Strategy**

Protecting data is an explicit goal of Best-in-Class organizations. The need for sharing data is growing both inside organizations and between organizations. Unless organizations are intentional about their data protection strategies, policies, and enforcement, unsecured file transfers pose a serious threat both from a potential loss of sensitive data as well as from failure to meet data protection regulations criteria.

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

"It seemed really easy when we looked at secure file transfer four years ago but the impact of data movement is much more complex. We're a big entity. We deal with big banks, mom and pop banks, and credit unions. We want to make things easy for our customers but there is no standardization across our customer base. Each one does it their own way and we need to be able to accommodate them all.

"Once we started to encrypt files we realized we had problems with managing the encryption keys. Trying to transfer confidential data can feel like we were trying to put a padlock on a car door - the design wasn't there to begin with and there's no easy way to do it. There's a lot of finger pointing. You need to ask 'Who's responsible for the transfer?' and 'Who's in charge of managing encryption keys?'"

~ CIO, \$70B Financial Services Organization

## Chapter Two: Benchmarking Requirements for Success

Selecting the appropriate secure / managed file solution(s) for an organization's current data transport needs is usually not simple. Because data protection regulations touch virtually every organization, keeping file transfer under the explicit rubric of data protection policies is paramount. The emergence of newer, robust solutions may mean that organizations can turn to more cost-effective alternatives. With the volume and diversity of file transfers on the rise, organizations need to find flexible, scalable, affordable solutions that will integrate easily into their work flows, staying within existing policies to the extent possible.

### Case Study — Large Commercial Bank

The manager of applications systems of a Best-in-Class organization, a multi-billion dollar commercial bank in the mid-west United States, indicated that they have been doing file transfers with their customers for a number of years. The company feels that the file transfer market is maturing and as a result, a couple of years ago the company sought to replace their costly file transfer solution. The manager of application systems for the company was pleased that they were able to find something more robust, more flexible, and less costly than their incumbent system.

“We needed something that would work with our existing work flow. This allows people to come in by different mechanism and it’s very flexible so that we can make changes quickly and easily. We need flexibility not only in how the solution faces the Internet, but we need flexibility in the components on our internal server. We take advantage of the post-processing that it enables. We were looking for something robust and reliable, and price was a consideration. We found it,” said the manager of application systems.

He further commented that the banking industry as a whole is being pushed toward significantly reducing paper and paper processing, for example, by replacing the exchange of physical checks with the electronic exchange of images of checks – not something they did until relatively recently.

### 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

### Fast Facts

- √ **63%** of Best-in-Class companies have integrated their secure file transfer system with AD, LDAP, ODBC or another access control database versus 26% of Industry Laggards
- √ **75%** of Best-in-Class companies require file recipients to authenticate themselves

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>	Consistent policies for sending files		
	89%	61%	50%
	Consistent policies for receiving files		
	74%	49%	45%
	Information classified by requirements for confidentiality, integrity and availability		
	78%	49%	41%
	Consistent policies for data at rest		
	61%	45%	43%
	Information grouped by the business process it supports		
	53%	40%	31%
<b>Organization</b>	Responsible executive or team with primary ownership for data protection		
	89%	73%	47%
<b>Knowledge</b>	Reporting all file transfer activity		
	61%	25%	22%
	Centralized collection, normalization and correlation of security and compliance information		
	61%	31%	25%
	Real-time notification of policy violations		
	39%	16%	16%
	Identified source (channel) of data loss incidents		
72%	35%	30%	
Identified source (user) of data loss incidents			
	74%	35%	24%
<b>Technology</b>	Secure File Transfer solution		
	83%	60%	53%
	Managed file transfer service		
	76%	31%	23%
	Integration of file transfer system with AD, LDAP, ODBC or other access control database		
	63%	40%	26%
	Automatic retry after transmission failure		
79%	69%	45%	
Authentication of file recipient			
75%	53%	47%	
<b>Performance</b>	Financial impact of data loss incidents		
	42%	18%	17%
	Effective measurement of total costs associated with protecting data		
	22%	18%	17%

Source: Aberdeen Group, September 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 reveals a spectrum of capabilities and enablers that the Best-in-Class leverage to a greater extent than do other organizations.

### Process

Policy, methodology, consistency. Whether it's corporate security policies or regulatory compliance, organizations need to identify and classify their data by requirements for confidentiality, integrity, and availability, grouped by the business process it supports. Core data protection policies need to be incorporated into explicit policies for sending and receiving files. Many organizations see file transfer usage coming from disparate entities within the organization. It behooves these organizations to look at the whole and address emerging needs as well as long-standing ones. Chances are there's better, easier to use, more secure, more powerful technology available at a lower cost than many legacy environments organizations have yet to realize.

### Organization

Ultimately organizations need to designate individuals or teams responsible for data transmission and protection and all the details that have to be addressed. If employees are encrypting files, who's responsible for key management? If employees are transferring files out of the organization in any number of ways, what safeguards do you have in place to protect sensitive data and who's in charge of making sure these safeguards work?

### Knowledge Management

Ironically, outside vendors might know more about the files people in your organization are sending than you do. In a world where file transfer is available on the web and requests to IT for an FTP account take time, chances are data is being sent without formal oversight. Organizations need to know and prove that they're in control of the data for which they are responsible.

### Technology Enablers

File transfer - and the disruptive innovation around it - is changing business process, productivity, and profitability. Brittle protocols are giving way to robust solutions that protect the organization and the data, provide functionality to business users and technologists alike, give management visibility that can translate into reliability, and enable collaboration throughout the organization's value chain.

The following are some of the elements that start to differentiate solutions and why they are important:

- Solutions that integrate directly into Active Directory, LDAP or an access control database where users are already grouped by role

have the advantage that file transfer policies can be built on established roles without needing to define them in the file transfer solution itself.

- Many solutions offer integration into email systems, automatically or intentionally requesting that large files are stripped out of email, and are stored securely on a server with a secure link delivered in the email. The recipient downloads the file from the secure server. Additionally, being able to access the contact database associated with the user's email client can mean that transferring the file to the recipient can be as easy as sending email.
- Smooth business processes will require integration with key applications within an organization as well as with key applications from the recipient organization. Typically file transfer solutions need to integrate with work flows, with workload management, job scheduling, automation tools and systems management. Architectures that facilitate these kinds of integration - use of open standards and support of service-oriented architectures - can go a long way toward the rapid integration of new partners / customers / suppliers.
- Solutions need to integrate into existing authentication solutions or provide authentication mechanisms as part of assuring safe delivery. Checkpoint restart - the ability to restart a transfer at the point of failure, delta transfers - transfers that transfer only what's different from the last transfer, automatic retry after transmission failure, guaranteed file delivery, and notification of failed delivery are all available to help organizations know that files successfully reach their destination.
- Often data being transferred needs to undergo some sort of pre-processing before its sent or post-processing on arrival or both. Some solutions facilitate the incorporation of the processes under the rubric of the file transfer.
- Some organizations need the ability to blind label their file transfer solutions to maintain the look and feel of their brand and corporate presence, and some solutions are easily customized and offer this capability out of the box

Add to these capabilities the file transfer accelerators and file transfer itself is taking a quantum leap.

### **Performance Management**

To understand the importance of protecting data as well as the potential cost-savings associated with using secure / managed file transfer, organizations need to measure the financial impact of data loss incidents, the costs of protecting the data, and the potential savings available by replacing shipping and courier services with electronic file transfer.

### Aberdeen Insights — Technology

Over the last 15 years email went from a specialized communication used between a handful of government agencies, technology vendors and universities to a ubiquitous channel of communication widely acknowledged as mission critical for businesses everywhere.

Email was never designed to transport huge files securely or guarantee their delivery, yet huge files are the coin of the day. The technologies emerging to bridge the gap not only in email functionality but in traditional file transfer solutions are really a call to action for organizations to scrutinize their usage of large files - now and in the foreseeable future - and to create and enforce acceptable use policy around file transfer.

It is insufficient to disallow ad hoc file transfer. Lack of adequate, available, usable, auditable file transfer mechanisms will stifle business and compromise the organization as, more often than not, users finding that the tools they have available to them are inadequate to the task at hand, will find free or cheap alternatives readily available on the web.

The advances in secure / managed file transfer are game changing and organizations may find that the solutions available to them today can profoundly improve their security, productivity, process, and cost savings.

## Chapter Three: Required Actions

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

### Laggard Steps to Success

---

- Laggard organizations need to find an appropriate **managed file transfer service** or solution. Putting all file transfer activity under management helps organizations to enforce policies, ensure compliance, effectively deliver and verify delivery of data, and meet service level agreements. Only 23% of Laggard organizations use managed file transfer services versus 76% of the Best-in-Class.
- Laggard organizations need to implement mechanisms that force file transfer receivers to **authenticate** themselves. Without this, there's no way to verify who actually accesses the file once it's sent. Only 47% of Laggard organizations authenticate the file transfer receiver versus 75% of Best-in-Class organizations.
- Laggard organizations need to implement mechanisms to **automatically retry** the file transfer on failure. Without automatic retry, processes fail and often go undetected or require manual intervention. Only 45% of Laggard organizations use automatic retry versus 79% of Best-in-Class companies.

### Industry Average Steps to Success

---

- Organizations that fall into the Industry Average class need to create and enforce **consistent policies for both sending and receiving files**. Compared with the Best-in-Class (89% have consistent policies for sending files and 74% have consistent policies for receiving files), only 61% of the Industry Average have consistent policies for sending files and only 49% have consistent policies for receiving files. Without these policies and their enforcement, organizations cannot appropriately protect their data and prove compliance.
- Key to understanding what data must be protected and how it can be safely shared is **classifying information by requirements for confidentiality, integrity and availability**. Seventy-eight percent (78%) of the Best-in-Class do this compared with only 49% of the Industry Average.
- Understanding that file transfer is a potential channel for data loss, organizations need to implement solutions that systematically look at all channels and make sure that data is protected across them all. Compared with the Best-in-Class for which 67% have **systematic implementation / rollout of data protection solutions**, only 32% of Industry Average organizations are actively pursuing this path.

### Fast Facts

- √ 79% of Best-in-Class organizations automatically encrypt file transfers
- √ 79% of Best-in-Class companies automatically alert an administrator on file transfer, file transfer failure or on file transfer policy violation

## Best-in-Class Steps to Success

- Best-in-Class companies can improve their data protection by implementing **real-time notification of policy violations**. Although significantly ahead of Industry Average and Laggard organizations, only 39% of Best-in-Class companies have adopted this strategy, leaving a lot of room for improvement.
- To the extent possible, Best-in-Class organizations can benefit by **implementing automatic enforcement of policy and remediation of policy violations**. Currently only 37% of the Best-in-Class have automatic enforcement and remediation, yet they are significantly ahead of the Industry Average (18%) and Industry Laggard (16%) organizations.
- Best-in-Class organizations should **look at their overall architecture for extending secure / managed file transfers across their ecosystems**. As they expand to engage with more partners, customers and suppliers, integrating with key external applications, they may be best served by a service-oriented architecture that can make integrating with new partners quicker and less onerous.

“Everybody needs to transfer more and more files, bigger and bigger files, with less and less technical skills. We tried doing FTP for a while but folks in litigation support wanted something that was coherent company wide that would work for both technical and non-technical people. We’re one of the largest international law firms with 10 offices around the world. We wanted something customized to have our look and feel. We’ve been very happy with the support we’ve gotten to implement and roll things out in ways that work for us.”

~ IT Manager,

International Law Firm

### Aberdeen Insights — Summary

Secure / managed file transfer is rapidly becoming a ubiquitous need - both between organizations and within organizations, both for regularly scheduled data transmission and for ad hoc collaboration - between partners, suppliers and customers everywhere.

Because virtually every organization has sensitive data for which it is responsible (for example, its employee social security numbers), organizations need to understand file transfer as a conduit for moving that sensitive data. Without adequate controls, organizations leave themselves needlessly vulnerable and potentially liable for data breaches.

However, well beyond the needs of data protection, file transfer is core to business process, and ensuring and improving business processes can lead to cost savings as well as better customer satisfaction and retention.

The need to transfer files to new entities and new devices including transferring files directly to mobile devices is part of the pent-up demand vendors are scrambling to provide.

Given the nature of conducting business in the electronic age, file transfer is rapidly becoming as necessary as email to the effective functioning of an organization. To the extent its deployment is seamless, its user interface easy to use, and its data protection and file transfer management is comprehensive, the sooner it will be acknowledged as the mission critical application that it is.

*Send to a Friend* 

## Appendix A: Research Methodology

Between August and September 2008, Aberdeen examined the use, the experiences, and the intentions of more than 130 enterprises using secure file transfer in a diverse set of enterprises.

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

Responding enterprises included the following:

- *Job title / function:* The research sample included respondents with the following job titles: C-level management (24%); EVP/ Director (24%); IT manager or staff (22%).
- *Industry:* IT consulting and services (20%); finance/ banking / accounting (18%); software / hardware providers (11%).
- *Geography:* The majority of respondents (63%) were from North America. Remaining respondents were from the Asia-Pacific region (10%) and Europe (19%).
- *Company size:* Twenty-six percent (26%) 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 50% of respondents were from small businesses (annual revenues of \$50 million or less).
- *Headcount:* Forty percent (40%) of respondents were from small enterprises (headcount between 1 and 99 employees); 14% were from midsize enterprises (headcount between 100 and 999 employees); and 46% of respondents were from large 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

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

- √ The degree to which secured/ managed file transfer is deployed in their operations and the financial implications of the technology
- √ The structure and effectiveness of existing secure / managed file transfer implementations
- √ Current and planned use of secure / managed file transfer to aid operations
- √ The benefits, if any, that have been derived from secure file / managed transfer initiatives

The study aimed to identify emerging best practices for secure file transfer usage and to provide a framework by which readers could assess their own management 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><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, September 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><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, September 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, September 2008

## Appendix B: Related Aberdeen Research

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

- [2008 Email Security Report](#), August 2008
- [Best Practices in Choosing and Consuming Managed 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
- [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](http://www.Aberdeen.com).

Author: Carol Baroudi, Sr. Research Analyst, 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. 043008a