

Secure File Transfer as a Core Business Process



an Osterman Research white paper
sponsored by

Accellion ™

Introduction

Physical delivery of sensitive data is fraught with risk; for example:

- Bank of America announced in 2005 that it had lost tapes that contained the personal information for 1.2 million individuals.
- The personal information for 3.9 million CitiFinancial customers was lost by a courier service.
- A thief stole a safe that contained data tapes from Arizona Managed Care Company – the data tapes contained sensitive data, such as medical histories and Social Security Numbers.

These examples point out the risk than any organization faces when it physically ships sensitive data, since even if courier services deliver virtually all of their packages successfully, a large number of shipments – including some that contain sensitive data – will be lost. Many organizations are simply not aware of the risk that they face when shipping sensitive information, not least of which is the risk from simply leaving packages unattended in a shipping department or outside an office door. This risk is not only from the loss of the data itself, but also from the loss of reputation that an organization might face as a result of losing data, the cost of notifying customers about the loss and the like.

One way to mitigate this risk is to develop secure, ad hoc file transfer capabilities as a core business process. This white paper discusses how new solutions are needed to accomplish this goal.

The Problem With Conventional File Transfer

Customer names, contracts, legal correspondence, presentations, business plans, sales reports, new product designs and loan applications are all examples of information for which no company would want to lose control. However, this information is routinely exposed to loss when shipped.

Physical delivery of sensitive information is a costly and cumbersome process that can take days to complete. Further, it offers less security than many people might realize,

Many organizations are simply not aware of the risk that they face when shipping sensitive information, not least of which is the risk from simply leaving packages unattended in a shipping department or outside an office door.

since there are numerous points at which a package can be intercepted.

An alternative to physical delivery is email, which offers several advantages compared to physical delivery, such as ease of use, much lower cost and dramatically faster delivery times. However, the downside of using email for transferring files – particularly large ones – is that servers can be overloaded and drag down the performance of a messaging system.

The downside of using email for transferring files – particularly large ones – is that servers can be overloaded and drag down the performance of a messaging system.

The Use of FTP Servers

Some organizations have deployed FTP servers for sending files. However, FTP was designed in an era when the security environment was much more benign. As a result, it is not uncommon for the same username and password to be shared among multiple users, which represents a potential and significant breach of security. Plus, basic FTP does not allow data to be tracked appropriately. While enhanced FTP systems, such as SFTP, FTPS and EFTP, represent significant improvements over conventional FTP, the requirement for specialized client programs to be installed on users' desktops makes this approach more cumbersome for users and IT alike.

People who upload files into FTP directories rarely remove them. The result can be a set of directories that contain hundreds of files with little information about when this information should be deleted, resulting in valuable digital assets left unprotected for extended periods where unauthorized users can access them. When IT must clean up an FTP server, the only information available to help them decide which files to keep is often just the file name, file type and date.

The Impact of Regulations

A variety of regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), the Food and Drug Administration (FDA) 21 CFR Part 11 and, most notably, Sarbanes-Oxley, require that companies prove that only the intended information was shared or exchanged (as required by HIPAA); that administrative controls are in place when electronic systems and records are used in place of paper or manual systems (as required by FDA regulations); or that business processes are auditable (as required by Sarbanes-Oxley). Conventional FTP is generally not compliant with these requirements, since it does not maintain a record of all

transactions -- business processes that rely on FTP to deliver information and other digital assets are not auditable and thus are not compliant with these regulations. The table below shows a few key regulations and their requirements.

Key Regulations and Requirements

Legislation	Vertical Segment	Requirement	Impact
Sarbanes-Oxley Act, Section 404	All industries	Requires public companies to verify that their financial-reporting systems have the proper controls, such as ensuring that revenue is recognized correctly. Requires testing and monitoring of internal controls via establishing, documenting, and auditing business processes.	Audit trails, authenticity, record retention
HIPAA	Health-care	Addresses security policies and procedures of insurance companies and providers regarding personal health information and services.	Record retention, privacy, protection, service trails
21 CFR Part 11	Life Sciences	Regulates life science and pharmaceutical companies involved in biotechnology and manufacture of medical equipment, food, and beverage concerning electronic and paper record retention.	Record retention, authenticity, confidentiality, audit trails
Department of Defense (DOD) 5015.2	Government	Concerns all defense-related government agencies' and contractors use of technologies relating to records.	Authenticity, protection, secure shredding
Securities and Exchange (SEC) Act Rules 17a-3 4 (17 CFR 240,17a-3,4)	Financial Services	Requires broker retention of sent and received communication, including interoffice memos, e-mails, sales training manuals, advertisements, and account records	Protection, audit trails Record retention, authenticity

In the face of traditional solutions like FTP and email failing to serve as adequate business tools for secure, ad hoc, large file transfers, it makes sense to consider a dedicated solution for business users.

New File Transfer Solutions

In the face of traditional solutions like FTP and email failing to serve as adequate business tools for secure, ad hoc, large file transfers, it makes sense to consider a dedicated solution for business users that has the following capabilities:

- Embedded business level security: security requirements extend beyond technical requirements like data encryption. They also include the need to authenticate the recipient and the ability to automatically manage each file and account life-cycle so that no confidential information is left exposed and no unauthorized user access takes place.

- Easy auditability and traceability: business practices, as well as legal and regulatory requirements, demand that companies have in place auditable business processes that often involves ad hoc file transfer.

The following table provides a comparison of various file transfer capabilities and a secure file transfer appliance offered by Accellion.

Among secure ad hoc file transfer solutions, it makes sense for any organization to consider the use of a File Transfer Appliance.

Comparison of Various File Transfer Capabilities

	FTP	Newer FTP (SFTP, FTPS, EFTP)	Email Attachments	Accellion Secure File Transfer Appliance
Suitable for ad-hoc file delivery	No	No	Yes	Yes
System account based	Yes	Yes	No	No
Login security	No	Yes	Possibly	Yes
Transport layer security	No	Varies	No	Yes (SSL)
Integrated virus scanning	Cumber-some	Cumber-some	Yes	Yes

Conclusion

Among secure ad hoc file transfer solutions, it makes sense for any organization to consider the use of a File Transfer Appliance (FTA) – a dedicated appliance that can solve the problems associated with conventional file transfer processes that are currently handled through email or FTP-based solutions. This type of appliance can benefit IT through its low maintenance and management requirements and can easily solve current file transfer problems. FTAs also solve the file transfer problem for end users by allowing them easy access to file transfer capabilities that include auditability and ease of use.

© 2005 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.