

Overcoming Key File Transfer Problems

An Osterman Research White Paper

Published September 2010

SPONSORED BY



Executive Summary

OVERVIEW

Organisations must transfer enormous amounts of information to support a wide range of business processes. These processes can range from the exchange of content between supply chain partners to claims information between healthcare providers and insurance companies to payments between governments and banks. These content transfers must take place in a timely manner and be managed in a consistent, compliant and efficient way.

However, many current file transfer processes are anything but timely, consistent or efficient. They often rely on use of the email backbone as the transfer mechanism and/or a hodgepodge of systems and out-of-date, insecure and hard-to-maintain scripts cobbled together to move information between business partners and others. Further complicating the problem is that individuals are often responsible for initiating or continuing the transfer of files with the result that file transfers are not conducted in a timely manner, if at all.

The result is that file transfer processes are not managed or monitored as carefully as they should be, security of the transferred content is lacking, and costs are higher than they need to be. This creates an environment in which corporate risk is increased and IT costs are unnecessarily high.

KEY TAKEAWAYS

Consequently, what Organisations need is a consistent and cohesive file transfer capability that will accomplish several things:

- Maintain visibility over the file transfer process, including logging, auditing and reporting on files over their entire lifecycle and maintaining chain-of-custody over important business content.
- Enforcing corporate policies for transferred files in the context of maintaining permissions for access and transfer of important business content, managing its security and managing bandwidth.
- Convert between disparate file types in an efficient, secure manner.
- Integrate file transfer processes with existing middleware and business applications so as to cause minimal disruption to the methods and procedures that already work within an organization.
- Support minimum service levels in order to minimize financial risks and maintain support for existing processes.
- Minimize corporate risks from non-compliance with the growing number of data governance requirements at all levels of government.

ABOUT THIS WHITE PAPER

This white paper discusses the problems with current file transfer processes and offers an overview of key elements that should be part of any enterprise-grade file transfer solution. This document also provides a brief overview of Ipswitch File Transfer, the sponsor of this white paper and its MessageWay offering.

Key Content Transfer Problems to Overcome

FUNCTIONAL PROBLEMS

For most individual users, email is the de facto and most common file transport mechanism in use today. Because of email's ubiquity, its ease of use and its reliance on industry-standard protocols, most users rely on the email infrastructure in their organization to send files of all sizes and types. Osterman Research surveys have shown, for example, that about 20% of the emails sent during a typical day contain at least one attachment, and that more than 95% of the bits that travel through the typical email system consists of attachments.

The result of using email as the primary file transport mechanism is that these systems suffer under the burden of carrying so much content, largely because they were never designed to do so. IT labor, hardware and software costs are all driven up as a result because more effort must be devoted to adding storage and addressing problems resulting from the transfer of such large quantities of files. Additional problems result from the fact that there is no guaranteed delivery of content in the vast majority of email systems; content is not encrypted in most cases, resulting in potentially significant security problems; and auditability of content sent through is, at best, difficult and time-consuming.

FILE MANAGEMENT PROBLEMS

However, users' application of email as their primary file transport mechanism for critical business content creates issues that represent only a small portion of the overall file transfer problem in most organisations. Using automated and manual systems, many organisations exchange large quantities of structured and unstructured data for transaction processing, for sharing information up and down the supply chain, or for processing insurance claims, to name but a few of the myriad applications for file and other content transfer.

A variety of systems are often employed to exchange this data, often resulting in incompatibilities between different file formats and with a lack of centralised control over how data is sent, translated and managed on a long-term basis. For manual content transfer processes, many organisations use legacy FTP systems that represent enormous security holes because the content on these systems is not managed properly and because many users – who typically use these systems infrequently – will often share login credentials. Many employees will use a growing variety of file-transfer systems over time that, although they may function well in sending files, are not managed in a centralised way. Other employees will turn to personal Webmail systems to send corporate content, resulting in loss of data security and an inability to manage content according to corporate or other policies. Still others will send it via overnight courier – in printed form, burned to a CD-ROM or DVD ROM or on a USB stick – leading to additional

Overcoming Key File Transfer Problems

data management problems and potential loss of physical media. Other tools used to send content include external hard drives, personal smartphones, non-sanctioned file-sharing Web sites that are outside the control and audit processes of the company.

The result is that files are not managed properly:

- **Content is not tracked throughout its entire lifecycle**
This is a long-term problem for many types of data, since a growing proportion of content must be maintained for several years.
- **Chain-of-custody is not maintained properly**
This results in potential legal and regulatory problems, particularly for organisations that serve heavily regulated industries like financial services, healthcare and energy.
- **Translation becomes cumbersome**
Transformation steps between different file and Electronic Data Interchange (EDI) formats introduces the creation of intermediate files and increases the potential for losing visibility of critical business content.

The consequences of these problems are that organisations that operate a haphazard collection of content transfer solutions lack visibility into the file transfer and management process, and they lack the ability to impose consistent standards for file transfer across all parts of the organisation.

CORPORATE GOVERNANCE PROBLEMS

The results of such poor data governance can include a number of quite negative consequences, including a failure to fully comply with a regulator's demands during an audit, charges of evidence spoliation during a legal action, an inability to comply with corporate or industry policies for data governance, or loss of corporate reputation.

For example, organisations' poor data governance practices can result in their running afoul of a large and growing number of regulatory requirements, among the most important of which for content management are:

- **Sarbanes-Oxley Act of 2002**
The Sarbanes-Oxley Act of 2002 obliges company officers to report their internal controls and procedures for financial reporting and requires auditors test the internal control structures.
- **Payment Card Industry Data Security Standard (PCI DSS)**
PCI DSS encompasses a set of requirements for protecting the security of consumers' and others' payment account information.
- **Basel II**
Part of the Basel Accords, Basel II is focused on protecting against financial problems in the banking industry and includes a number of specific requirements on banks to prevent financial irregularities and undue risk.
- **The EU Data Protection Directive**
EU Data Protection Directive (also known as Directive 95/46/EC) is a directive adopted by the European Union designed to protect the privacy and protection of all personal

Overcoming Key File Transfer Problems

data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data. Directive 95/46/EC encompasses all key elements from article 8 of the European Convention on Human Rights, which states its intention to respect the rights of privacy in personal and family life, as well as in the home and in personal correspondence.

- **Gramm-Leach-Bliley Act (GLBA)**

GLBA requires that financial institutions protect information collected about individuals, including names, addresses and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers.

- **The Data Protection Act**

The Data Protection Act is mandatory and is the main piece of legislation that governs the protection of personal data in the UK. All organisations that hold or process personal data must comply. Compliance with the Act is regulated and enforced by the Information Commissioner's Office.

- **Model Requirements for the Management of Electronic Records (MoReq)**

MoReq is a specification, originally developed in 2001, that defines the functional requirements for the manner in which electronic records are managed in an Electronic Records Management System. MoReq has been used widely in Europe and has been updated with MoReq2.

- **Worldwide acts and agencies**

Most other nations impose stringent requirements, as well, particularly the United States which has a number of further acts including Personal Information Protection and Electronic Documents Act (PIPEDA), Health Insurance Portability and Accountability Act of 1996 (HIPAA) and International Traffic in Arms Regulation (ITAR). Among the many agencies that impose requirements on how data is managed in the US include Securities and Exchange Commission, the Financial Industry Regulatory Authority, the Occupational Safety and Health Administration. The majority of EU companies have their own data act.

Legal problems can also result from poor data governance, including an inability to perform adequate early case assessments or satisfy e-discovery requirements because data is not accessible or in a form that can be easily processed, or an inability to place legal holds on data if and when required.

THE BOTTOM LINE

The ultimate result of poor data governance arising from inadequate file transfer and data management practices is that:

- Overall corporate risk is higher than it should be.
- IT and business costs are higher than they should be.

The Top Ten Things to Look For in an Enterprise Content Transfer Solution

To address day-to-day content management problems when sending files, and to address the larger issues associated with corporate risk and overall IT costs, organisations should implement a robust content transfer solution. Instead of relying on email and/or a disparate collection of alternative transfer methods as the file transport mechanism for business-critical content, an enterprise-grade content transfer system should be deployed that offers the following capabilities:

1. **Data translation between diverse file constructs**

Because a wide variety of file types are exchanged between organisations – including EDI, ERP, proprietary formats, and desktop application formats – an enterprise-grade file transfer solution should translate between diverse file types automatically and in as close to a real time manner as possible. The file transfer system should not create intermediate documents during the transformation process that can introduce additional security or audit problems.

2. **Visibility during entire lifecycle**

It is critical that any enterprise-grade file transfer system be able to monitor, report and audit on content over its entire lifecycle. Because some documents must be maintained actively for several years, the file transfer system should be able to monitor the location and status of this content for as long as necessary for purposes of regulatory, legal and corporate compliance – maintaining chain-of-custody tracking as a file moves from system to system or from company to company is absolutely essential. For example, a robust file transfer solution should be able to identify when content transfers are late or when they never came through so that one or more parties can avoid financial penalties or other consequences.

3. **Integration with existing middleware and business applications**

Ideally, any enterprise-grade file transfer solution will be able to integrate with the systems and processes already in place in an organisation for two reasons. First, a robust file transfer solution should be able to absorb existing IT process flows instead of requiring a rip-and-replace of processes that have already been demonstrated to work effectively. Secondly, a file transfer system that requires too radical a paradigm shift for those charged with managing or using it simply will not be used, regardless of how much pressure IT or business units place on those charged with employing the new system.

4. **Granular control over file transfers**

It is important that any file-transfer solution offer granular control over file transfers, such as a file transfer that takes place outside of a normal business process. For example, there may be a unique situation that a normal business process does not accommodate. An enterprise-grade file transfer solution should be able to accommodate this type of transfer according to the unique requirements of this one-off situation.

5. **Content validation**
Any file-transfer system should be able to validate incoming content so that corrupted or non-compatible data is not provided to processes or systems.
6. **Support for multiple operating systems**
A file-transfer system should support multiple operating systems and platforms – including all those that a company and business partners might need to support today or in the future.
7. **Support for virtualized environments**
Any file transfer solution must support virtualized environments. Because virtualization is becoming widely used as a means of reducing IT hardware costs, power costs and data centre footprint, it is imperative that any file transfer solution be able to integrate with and operate in a virtualized environment.
8. **SLAs that will permit organisations to manage file transfers efficiently, effectively and in a timely manner**
SLAs are a critical consideration in any business-critical file transfer process, since both IT and business users must be given assurance that content is sent and received in a timely manner. This is a very important consideration for time-sensitive business processes that require on-time delivery of content as part of an overall process.
9. **The ability to drive cost out of the file transfer process**
Key to any system is its ability to drive down costs and enterprise-grade file transfer solutions are no exception. Because many current file transfer solutions – whether automated or manual – are highly inefficient, a robust file transfer solution can be of significant benefit in driving down the direct cost of file transfers. Further, because they can make existing processes more efficient, a good file transfer solution can provide ancillary benefits, such as reducing the cost of storage.
10. **The ability to manage file transfer volumes today and for the next several years**
Any enterprise-grade file transfer solution should be implemented with the long term goal of being able to manage current and future content transfer capabilities. This means that a robust solution should be able to scale to many times the current content transfer load in order to accommodate enormous increases in file transfers that might occur in the future, as well as to accommodate large spikes in file transfers.

Summary

Large organisations– and many smaller ones – are increasingly dependent on the transfer of disparate types of information to support a variety of business processes. Many organisations address their content-transfer requirements in a haphazard way using a variety of unmanaged and unmonitored, automated and manual approaches. This results in a loss of content security, loss of visibility into file transfer processes, an inability to

Overcoming Key File Transfer Problems

cleanly convert content types as needed, and an inability to comply with corporate governance requirements.

What organisations need, therefore, is a way to manage their content transfer processes in an efficient manner that allows:

- Complete, end-to-end management of content over its entire lifecycle.
- Enforcement of corporate policies, including authentication rules user permissions, security policies and other requirements.
- The ability to transform any file type to any other file type.
- The ability to integrate file transfer with existing business processes.
- SLAs that will guarantee timely delivery of content.

The ultimate goal of any file transfer system is to mitigate corporate risk and drive down IT costs to the greatest extent possible.

About Ipswitch MessageWay

MessageWay solutions enable companies to manage, customise and govern all aspects of message, file and data exchange. MessageWay is data centre-ready, highly scalable, service-oriented and completely integrates with existing middleware and business applications. MessageWay delivers data translation, validation, file life-cycle tracking and advanced analytics and is proven to handle extreme volumes of data transfers.

Industry experts such as Gartner continue to say that 80% of B2B e-commerce is actually electronic file exchange. The same experts project that future file exchange volumes will continue to grow, both in numbers of files and size of payload. With so much riding on their file transfer programs, CIOs are already re-evaluating their transmission infrastructure to ensure they are able to meet current and future needs.

But while the secure exchange of files with trading partners is important, it's just the tip of the iceberg. The most difficult segment of an electronic file exchange occurs after a file arrives on the edge of the network. Once a file is safely stored behind the firewall, it is subject to multiple transfers across multiple servers – and possibly multiple domains – in order to prepare it for delivery to its final destination. A Managed File Transfer (MFT) solution that fails to deliver on this key requirement is only doing half the job.

As a result, an increasing number of enterprises are turning to MFT with Advanced File Services to reduce costs and eliminate the risks inherent in other methods of file exchange and transformation. Ipswitch MessageWay technology and services provide a strategic AFS solution that completely meets these objectives through secure, reliable, and scalable communications over open protocols, full control and visibility of all file exchange traffic, efficient mapping of file or EDI formats, and a high degree of integration with related technology.

Overcoming Key File Transfer Problems

© 2010 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 or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.