Why You Need an Intelligent File Transfer Solution

An Osterman Research White Paper

Published January 2009

Why This White Paper Will Be Worth Your Time

Email is the default file transport system in most organizations: an Osterman Research survey conducted in 2008 found that nearly one-third of emails contain attachments and 95% of the information that flows through email systems in the typical organization is attachments.

EMAIL WAS NEVER DESIGNED TO SEND LARGE FILES

However, while email is a very easy way for users to send files, email systems were never designed to handle this load. When users send large attachments through email, it can create a variety of problems, including:

- Poor email server performance, including slow mail delivery
- Higher costs for storage
- Slower backups and longer restores
- The risk of losing sensitive information

Also, when file size limitations prevent users from sending large files through email, they often will use overnight courier services or FTP as alternatives, resulting in higher costs and/or greater security risks.

MOST DO NOT USE ENCRYPTION

Compounding the security problems associated with current practices is that encryption is normally not used when sending files through email. Most employees do not know how to use encryption or they might not even have access to it. Many who can use encryption don't use it because it is too complex. Some users employ third-party, hosted services to send files securely, but most IT decision makers want data stored and managed behind the firewall to maximize security.

Now, add to all of this the critical need to maintain good corporate governance practices. While financial services firms have always been subject to strict governance requirements as dictated by the SEC, FINRA, the New York Stock Exchange, Gramm-Leach-Bliley and other regulatory and quasi-regulatory entities and statutes, all firms in all industries must practice good corporate governance, albeit to varying degrees. One of the results of the current financial problems we're experiencing will be greater government oversight for businesses of all types – expect there to be much more emphasis on good corporate governance practices during 2009 and beyond.

> Expect there to be much more emphasis on good corporate governance practices during 2009 and beyond.

ORGANIZATIONS NEED AN INTELLIGENT SOLUTION

What organizations need to overcome all of these problems and to exercise good corporate governance is a solution that will allow users to send any file:

- With minimal or no training
- With little impact on their normal business processes
- Securely
- With robust auditing capabilities, and
- Independently of the email system

This white paper discusses the problems associated with the common practice of sending content through email systems, and it provides information on Biscom Delivery Server, an intelligent attachment management solution that directly addresses these problems.

Problems With the Status Quo

Although many organizations have deployed FTP systems to send large files, email is actually the de facto file transport mechanism in most organizations. Email is almost universally deployed, it is very easy to use and, because almost all email systems in corporate environments adhere to corporate standards, users are normally confident that files that make it through to their destination can be read by the recipient.

However, email, when used as a file transport system, is fraught with problems, including the following:

- **Files sizes are getting larger**
  As a result of increased use of attachments, larger attachments and greater use of multimedia content, the sizes of files that are sent through email are getting larger over time. A survey conducted by Osterman Research in 2008 found that 29% of all emails sent in corporate environments contain attachments. Of these attachments, 19% are greater than five megabytes and 6% are greater than 10 megabytes. As a result, about 95% of the bandwidth used by email systems is accounted for by just the attachments.

- **Storage is getting more expensive**
  As a corollary to the point above is the fact that email-related storage is becoming significantly more expensive as a result of increased storage requirements. For example, using the Exchange 2007 Mailbox Server Role Storage Cost Calculator provided by Microsoft, storage costs for a 2,000-, 4,000- and 20,000-mailbox environment will be as shown in the following tables:

Exchange Storage Costs
2,000-Mailbox Environment

Configuration	Production Lifecycle Power-Cooling Cost	Total Disk Cost	Total Cost	Lifetime Cost per Mailbox
Storage Area Network (SCC)	$17,685	$88,280	$105,965	$52.98
Direct-Attached Storage (CCR)	$11,767	$22,880	$34,647	$17.32

Notes: assumes 1Gb+ mailboxes, high-availability model, two database copies per mailbox server via continuous replication, production lifecycle of three years.

Exchange Storage Costs
4,000-Mailbox Environment

Configuration	Production Lifecycle Power-Cooling Cost	Total Disk Cost	Total Cost	Lifetime Cost per Mailbox
Storage Area Network (SCC)	$35,371	$176,560	$211,931	$52.98
Direct-Attached Storage (CCR)	$23,533	$45,760	$69,293	$17.32

Notes: assumes 1Gb+ mailboxes, high-availability model, two database copies per mailbox server via continuous replication, production lifecycle of three years.

Exchange Storage Costs
20,000-Mailbox Environment

Configuration	Production Lifecycle Power-Cooling Cost	Total Disk Cost	Total Cost	Lifetime Cost per Mailbox
Storage Area Network (SCC)	$88,427	$441,400	$529,827	$26.49
Direct-Attached Storage (CCR)	$58,834	$114,400	$137,234	$8.66

Notes: assumes 1Gb+ mailboxes, high-availability model, two database copies per mailbox server via continuous replication, production lifecycle of three years.

Osterman Research has found that email-related storage requirements are growing at roughly 30% per year. This means that for every terabyte of storage needed today, nearly 2.5 terabytes of storage will be required in just three years. Even with declining acquisition costs for storage, total email-related storage costs are growing even more quickly and overall costs are rising.

- **Large files slow email server performance**
  Email was designed as a transport mechanism for small amounts of information per message, namely short messages as might be contained in a few paragraphs of text in an email message. Large attachments sent through email bog down email server performance, particularly when emails with large attachments are sent to multiple

recipients. The result is that email delivery slows and storage on email servers increases.

The impact of large attachments sent through email should not be underestimated. In multiple Osterman Research surveys over the past two-plus years, messaging-focused decision-makers in mid-sized and large organizations have reported that growth in storage is the leading problem in managing email systems – 60% of decision makers consider this to be a serious or very serious problem.

- **Many users cannot send files because of file size limitations**
  Many organizations impose limitations on the maximum size of files that can be sent or received through email in an effort to minimize the negative impact of large files on email server performance. For example, an Osterman Research survey conducted in 2008 found that 7% of organizations have an attachment size limit of five megabytes and 30% have a limit of 10 megabytes; only 4% of organizations surveyed have placed no limits on the size of emails that can be sent through email.

  While imposing such limitations is reasonable and necessary, it often leads to undesirable behavior on the part of users. This includes the use of expensive alternatives to email, such as overnight couriers or postal services; slower delivery of files if these physical alternatives are used; and use of personal Webmail accounts that have less restrictive file size limitations. While most of these alternatives drive up the cost of delivering large amounts of content and slow its delivery, they also result in reduced security as parcels are left outside office doors unattended waiting for pickup. Some users will employ FTP systems to transmit large files, but FTP has its own problems, including unmanaged file repositories and sharing of passwords, both of which impose additional security difficulties, and the involvement of IT resources to administer new users, directories, and permissions.

> An Osterman Research survey conducted in 2008 found that… only 4% of organizations surveyed have placed no limits on the size of emails that can be sent through email.

- **Lack of auditing capabilities**
  Few email systems provide native auditing capabilities that can provide guaranteed delivery of the content to the intended recipient or a notification email sent back to the sender, nor do they provide a true audit trail of file transfer activity. This results in a lack of information security for senders who cannot verify receipt of their content by the intended recipient. And many organizations require a way to track how and to whom information is disseminated for compliance requirements.

- **Lack of encryption**
  Further complicating the security problems associated with the status quo is that encryption is typically not used when sending large files (or even small ones) through

email. Most employees are not familiar with encryption technology and many simply do not have access to the tools that handle file encryption. While some users will employ commercial, hosted services to send files securely, most IT decision makers want data to be stored behind the firewall to minimize security concerns.

Content that is sent in clear text, such as email messages, result in a number of problems, including lack of compliance with legal, regulatory or corporate policies; potential breaches of client confidentiality; potential legal repercussions; loss of intellectual property; and, in extreme cases, loss of trade secrets.

Benefits of Secure, Managed File Transfer

A secure, managed file transfer system can resolve the issues associated with sending attachments through email and its alternatives, and can provide a number of important benefits for users and IT alike. Among these benefits are:

- **Built-in encryption**
  The encryption capabilities of a secure, managed file transfer system ensure that the integrity of the content is maintained from sender to recipient and that it will not be accessible by unauthorized parties. A properly designed file transfer solution will both encrypt the data in transit using SSL, for example, and will protect data at rest using file encryption.

- **Easing the burden on email servers**
  Secure, managed file transfer significantly reduces the load on email servers (particularly when large files are sent), allowing them to operate at peak performance so as to minimize message delivery times and maximize message throughput. Ultimately, this can result in organizations deploying fewer email servers and deploying more mailboxes per server, resulting in lower TCO for email.

- **Reduced email-related storage requirements**
  Significant reductions in email server storage requirements can be achieved through the use of secure, managed file transfer because content is offloaded from "live" email storage. This results in less IT time spent managing email server storage, better email server performance, shorter backups and faster restores after a server problem. This can also result in less email server downtime that leads to greater employee productivity.

- **Reduced email-related storage costs**
  As email storage requirements are reduced, email-related storage costs are also reduced accordingly. For example, using the data in the table above for a 20,000-mailbox organization, every 10% reduction in email storage will result in a nearly $53,000 savings in a SAN-enabled Exchange environment.

- **Less impact on network bandwidth**
  Secure, managed file transfer also results in less impact on bandwidth because most of

the content that would normally be sent through email is avoided. While notification is sent immediately, the actual download of the attachment occurs only on demand and is spread out over time, resulting in much lower impacts on network bandwidth.

- **True audit trails**
  Secure, managed file transfer provides true audit trails for each message sent, assuring both senders and recipients that their messages have been delivered securely and received by the intended party. Further, the ability to audit the delivery and receipt of messages is a key component in a sound corporate governance capability that allows organizations to be compliant with the growing array of governance requirements that they face currently and will face in the future.

- **Message retraction**
  A sound file transfer solution will allow a sender to retract a message once it has been sent, such as when the sender needs to send an updated attachment, remove a recipient from the original message or fix a recipient's address. Few email systems provide this type of retraction capability.

KEY FEATURES THAT SHOULD BE INCLUDED

Not all secure, managed file transfer solutions provide the complete list of capabilities that organizations should specify as they evaluate file-transfer alternatives. A secure, managed file transfer solution should include the following capabilities:

- **Ease of use**
  Because users may simply refuse to use systems that are difficult to use, particularly given the ease of use that most current email systems provide, a managed file transfer solution must fit well within the context of users' practices and experience level. Consequently, any secure, managed file transfer system should be very easy to use (including, ideally, drag-and-drop capabilities) and require only minimal training (or, ideally, no training at all).

> Any secure, managed file transfer solution should support the directory infrastructure already in place – most often an LDAP-based solution or Active Directory.

- **Secure reply**
  Recipients of content should be able to reply securely to messages they receive in order to maintain the security of the conversation. For example, a doctor that communicates Protected Health Information (PHI) to a patient must be assured that the patient responds securely, not in clear text which could result in a HIPAA violation.

- **Scalability**
  Any secure, managed file transfer solution should be as scalable as organizations need it to be and then some. A solution must handle not only today's volume of content, but also spikes in content delivery and future content delivery loads. A secure,

managed file transfer solution that does not scale properly will simply trade the problem of today's email delivery of large files for a different – but equally inadequate – solution.

- **Support for existing user directories**
  Any secure, managed file transfer solution should support the directory infrastructure already in place – most often an LDAP-based solution or Active Directory. This will allow more efficient content delivery and a single point of user management, roles management and permissions management. This is a big plus if users can access the global address list when addressing a new delivery.

- **No limitations on file size**
  A secure, managed file transfer solution should handle files of any size. While most files are not enormous, there are some specialized requirements to send very large files, including architectural drawings, graphic designs, manufacturing drawings, etc.

- **Robust integration capabilities using APIs**
  The ability to integrate a secure, managed file transfer system with existing systems is crucial in some applications. Users should be able to send files not only from email, but also from real-time communications systems, collaboration tools and any other system that users employ. Web services support and other platform and programming neutral API is best for the greatest breadth of support for both new and legacy applications.

- **Flexibility of deployment options**
  A secure, managed file transfer solution should run on the operating systems already deployed in the organization without requiring deployment of another operating system. Ideally, the solution should also not require any client-side installations, since doing so adds to the cost of the deployment and management of the solution, in addition to driving up help-desk costs. This would force IT to "learn" a new system that they may not be able to fix. Many hardware appliance vendors fall into this concern, as the IT staff is not familiar with the underlying hardware platform and operating system. Further, some appliances may be limited in scalability – simply adding a hard drive to an appliance may cost many more times that the actual cost of the new hard drive.

- **Robust management capabilities and data governance**
  Any secure, managed file transfer system should include the management capabilities needed to help IT and users do their work, including real-time tracking of content, return receipts, message recall, etc. Policy-driven and rules-based file transfer applications give administrators robust and granular control over proper access to data, and can help plug "data leakage" holes by restricting delivery of certain content. This includes policies like keywords, file sizes or file types (such as .EXE or .ZIP files) that will trigger automatic delivery by the file transfer system instead of via email. Policies should also allow restrictions to be placed on content delivery, such as restricting the sending of files to specific domains (i.e. a competitor's domain) and restrictions on the types of files that can be sent. It should also include automatic expiration and file

deletion schedules to prevent old content from cluttering up servers, and aligning with record retention policies.

- **Compatibility with virtualized environments**
Many organizations are migrating to virtualized environments to simply server management, reduce costs, reduce power consumption and to make IT staff more efficient. A file transfer solution should be compatible with leading virtualized platforms.

- **Support for Web services and a Software-as-a-Service model**
A secure, managed file transfer system should support a Web services model, as well as a hosted/SaaS model given the growing popularity of these delivery models.

- **Other capabilities**
Among the other capabilities that should be included in a managed, file transfer solution are:

    - Customization capabilities
    - Integration with the existing infrastructure, including network-attached storage and storage-area networks
    - A three-tier architecture for security
    - APIs for integration with existing/legacy applications, but also the ability to create new applications tailored to the organization
    - Checkpoint restart capabilities for large files

Summary

Email is the backbone of most organizations' communication infrastructure and an incredibly useful tool in its own right. However, email has also become the de facto file transport system for most organizations, a role it was never intended to play. As a result, large file transfers sent through email impede efficient email server performance, resulting in slow message delivery times, higher storage costs, slower backups and slower restores. In addition, security of the content sent through email servers can be compromised. If file size limitations prevent users from sending particularly large files through email, users find alternative methods to send their content, driving up costs and sacrificing security.

What organizations need is an alternative to the status quo: an attachment management capability that will allow efficient and secure delivery of content that will keep costs low and improve email server performance. BDS allows an organization to significantly improve file transfer processes, reduce network bandwidth, improve email server performance, mitigate the risks inherent in other delivery models and significantly reduce its IT costs.

About Biscom

Biscom was founded in 1986 and pioneered the fax server marketplace, providing mission-critical solutions to many of the world's largest organizations with its award-winning FAXCOM fax servers. In addition to enterprise fax server products, Biscom also offers hosted fax services, secure file transfer and messaging solutions, file conversion software, and document workflow and automation tools. The company is headquartered in Chelmsford, Massachusetts.

ABOUT BISCOM DELIVERY SERVER

Built from the ground up to be a superior secure file transfer solution for today's file delivery needs, Biscom Delivery Server is an enterprise managed file transfer application that enables users to deliver documents, files, and messages in a simple and secure manner. With today's government regulations and compliance requirements, and an increased awareness and need for security, many existing file delivery methods are no longer suitable for sending information. BDS solves the issues surrounding email, FTP, and even overnight delivery services, by providing a simple way for people to deliver these critical files quickly and easily, all while maintaining a secure and trackable electronic package.

BDS SCALES FROM SMALL WORKGROUPS TO ENTERPRISES

BDS can be deployed as a workgroup solution that handles the secure communication needs of an internal department. For example, because of the sensitive nature of personnel records, the HR department may need a way to securely deliver medical, financial, and personal records to insurance agencies, healthcare facilities, and payroll services. In organizations that require multiple departments and large numbers of employees to lock down their communications, BDS can scale to support multiple sites, use directory services such as LDAP and Active Directory to manage users, and integrate with email systems for seamless operation that requires minimal user training. In addition, existing and legacy systems can take advantage of a secure file transfer server via the BDS Web services, Java, or .NET APIs.

As a platform neutral application, BDS runs on the hardware and operating systems that your organization already knows how to support. When the latest hardware platform is deployed in the organization, BDS can be moved easily to the latest and greatest server with minimal downtime. Because your IT staff is familiar with the hardware system, it can be maintained with the latest security patches and upgrades.

FLEXIBLE ARCHITECTURE

The multi-tier architecture provides your IT group with the capability to configure the application from a simple file transfer server to a fully redundant, load balanced set of servers that keeps your important data and files in highly secured parts of your network. BDS is also compatible with virtualized environments, can be customized to the organization's look and feel, and is flexible to match any existing security infrastructure that may already be in place.

EVERYTHING INCLUDED

BDS comes with everything you need to get started, as well as everything you need to scale it up when you're ready. Along with the primary server, BDS includes clients for Outlook, a desktop client, LDAP and Active Directory integration, and a Web interface with support for auto-complete, access to Microsoft Exchange's global address list, and drag and drop simplicity. Your data is safely encrypted in transit as well as at rest.