Why You Need a Better Way To Manage Email Attachments

An Osterman Research White Paper

Published September 2010

SPONSORED BY

yousendit™

OSTERMANRESEARCH

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com • www.ostermanresearch.com

Executive Summary

It goes virtually without saying that email is an incredibly useful tool. Originally designed as a means of sending bursty, temporary types of messages, email has become the primary communications medium in most organizations, the dominant method for sending electronic files of all types, and the primary repository for important business content in many organizations. Consider:

- Email is used 146 minutes per day by the average corporate email user – substantially more than the telephone, instant messaging and social networking combined[i].

- The typical user sends and receives 40,000+ emails every year.

- Despite the rapid growth of social networking, real-time communications and other tools, email use continues to grow.

- 61% of users employ their email solution as a repository of business-critical information[ii].

- Email is the primary method for sending attachments to others inside and outside the organization.

KEY TAKEAWAYS

The dependence on email as an attachment transport mechanism has created significant problems. Because 98% of email traffic consists of attachments, performance of email systems suffers and is manifested by slower message delivery and greater susceptibility to downtime. Other problems caused by the reliance on email for attachment transport include higher costs for storage and other infrastructure, additional IT labor devoted to managing the email infrastructure, an inability to track accurately if and how files flow through the email system, longer backup windows, longer restore times after server crashes, and an overall lack of control over much of the content that flows through email.

In short, what organizations need is a way to solve their attachment management problems while imposing little or no change on the way that users work and increasing IT's visibility into the process for compliance purposes. And, to do so as inexpensively as possible and in a way that reduces corporate risk.

ABOUT THIS WHITE PAPER

This white paper discusses the important requirement to implement an attachment management solution and why such a solution is needed in the first place. It also provides a brief overview of YouSendIt, the sponsor of this white paper, and their relevant attachment management solutions.

How Things Are Done Today

THE WAY FILES GET SENT IN MOST ORGANIZATIONS

Most email users employ their email client as the primary tool for sending files like word processing documents, spreadsheets, presentations and other content. There are several good reasons for this, including:

- Virtually all email systems are built on industry standards, providing users with almost total assurance that their emails can be received and opened by recipients (albeit without proof that their attachments have *actually* been received by the recipients, as discussed later in this report).

- Email is ubiquitous and available on a wide range of platforms (desktop client at work or home, laptop, browser, mobile device, etc.)

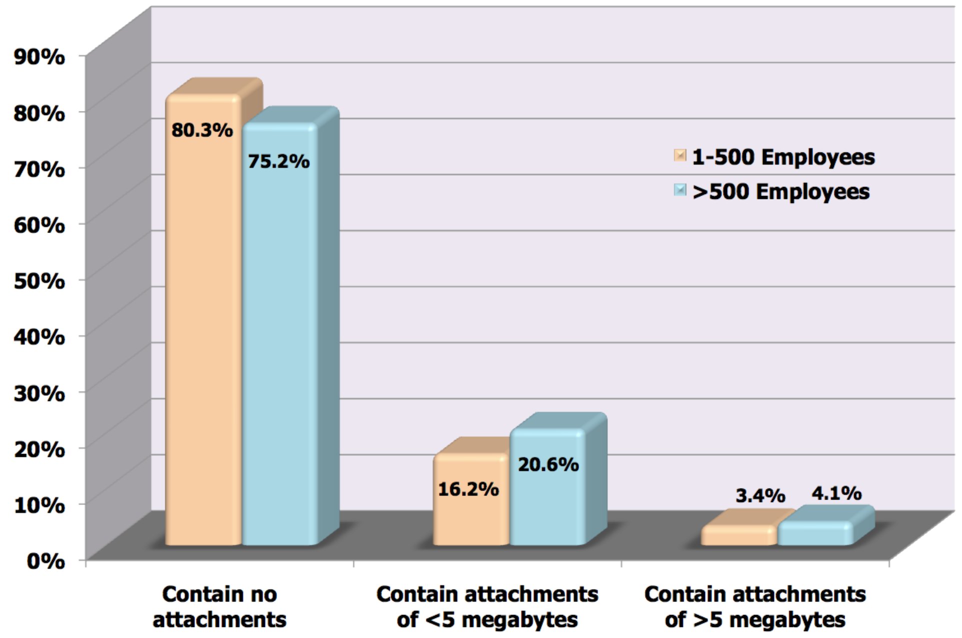
- Email is extremely easy to use and requires virtually no training in order to send attachments.

- Email has become the de facto method for sharing content with those outside of the organization because it is easy to use, ubiquitous, and because standards allow messages and attachments to be shared between virtually all email systems.

The result is that email has become the primary attachment transport mechanism in most organizations. While other tools continue to be used to send electronic files – such as corporate FTP systems, instant messaging, other real-time communication tools and physical delivery of CDs and DVDs – email is the primary platform that individuals use to send electronic content. For example, an Osterman Research survey found that of all of the content sent during a typical day – including paper and electronic content – 74% is sent through email.

As evidence of the critical role of email in sending electronic content is the following figure that demonstrates that 20-25% of all emails contain attachments[iii], a figure that is holding relatively steady over time.

Percentage of Emails With and Without Attachments



The Osterman Research survey from which this data came also found that the typical user in organizations of up to 500 employees sends and receives a total of 173 emails on an average day; users in larger organizations send and receive a total of 160 emails. What is particularly telling about this data is that while emails without attachments constitute 75-80% of the total *number* of emails that that are sent and received in corporate networks, emails without attachments account for only 1.3% to 1.7% of the total *volume* of content. In other words, attachments account for more than 98% of the bits that are sent through corporate email systems.

CONTINUING TRENDS IN ATTACHMENT TRANSFER

There are several important trends occurring in the context of how attachments are managed:

- Attachments are getting larger as users create more word processing documents, spreadsheets, presentations, PDF files, and other content. This is particularly true as the use of video increases for corporate presentations and related uses, and as consumer content authoring tools become more sophisticated.

- Employees are becoming more distributed and geographically separated as companies implement work-from-home policies in an effort to reduce the costs of rent and other expenses associated with providing employees with office space. The result is that employees who can no longer collaborate face-to-face instead rely more on the sharing of documents by email in order to collaborate on projects.

- Despite the growing use of alternatives to email – social networking, unified communications, Web conferencing, real-time communication and other tools – the use of email continues to increase. For example, an Osterman Research survey published in February 2008 found that users in organizations with up to 500 employees sent and received 129 emails on a typical day; users in larger organizations sent and received 140 emails[iv]. That means that email use in smaller organizations has increased by 34% in just over two years; in larger organizations email use has increased by 14% during this period.

- Another important trend in exchanging content is the growing importance of data security driven by compliance regulations, growing concerns over data leaks, and protection of intellectual property. As a result, IT needs greater visibility into who is transferring content and the types of content being sent.

- Related to the point above about IT needing greater visibility into content delivery is the need to recall content when needed, the ability to set timelines for availability of content, guaranteed delivery receipt for certain types of content and better security of information.

The bottom line is that email is being used more, email attachments are getting larger, and reliance on email as the transport mechanism for electronic content is increasing.

What's Wrong With the Way Things are Done Today?

Despite the utility of email as an attachment transport solution, there are seven basic problems with this status quo of file transport:

- **Email was never intended for large file transfers**
  Despite the ease with which files can be sent and received in email, it was originally designed as a medium for sending short messages, much like instant messaging. When email is used for transporting files, particularly large files, email server performance slows, message delivery can be delayed, and more infrastructure (servers, storage and bandwidth) are required over time. Additionally, finding content becomes more difficult with the result that things like e-discovery and regulatory compliance are made more difficult and more costly, increasing corporate risk of non-compliance.

- **Growing email storage is a serious problem**
  The growth of email storage and the problems related to it are a major problem for many email administrators. For example, in an Osterman Research survey[v] of decision makers in mid-sized and large organizations conducted in March and April 2010, various issues related to email storage were determined to be serious or very serious problems:

- Increasing message size (55% view this as a serious or very serious problem)
- Increasing backup and restore times (51%)
- Lack of messaging-related disk space (37%)
- Mailboxes are overloaded (35%)

The same survey found that email storage during the 12 months prior to the survey had increased a mean of 25.4%. At that rate of growth, in just three years storage requirements will increase by 97% in the typical organization.

The result of these problems is that costs are driven up because more storage is being deployed in corporate messaging networks, more IT labor is needed to manage email systems, and overall email system performance suffers. It is important to note that the issue is not the cost of storage itself – the cost of storage hardware is actually declining quite dramatically over time. Instead, the issue of storage is the cost of IT deploying and managing it – this can be anywhere from five to eight times the cost of the storage solutions themselves.

- **Content is normally sent unencrypted**
  The vast majority of emails are sent by users without any encryption, including the attachments that these emails contain. This not only increases the likelihood that sensitive or confidential information will be exposed to unauthorized parties, but it increases the risk of non-compliance with a growing variety of legal and regulatory obligations to protect sensitive data in transit. For example, 46 of the 50 US states now have data-breach notification laws, and two US states (Nevada and Massachusetts) have enacted statutes that require the encryption of certain types of data when sent to individuals in those states. Emails and attachments that are not encrypted can create enormous liabilities for an organization that suffers a data breach caused by unencrypted email being exposed or lost, even if the owners of that information do not suffer any harm as a result.

- **IT lacks control over externally sent content**
  Another important issue is that IT often lacks control over content that is sent outside of an organization, often because unsanctioned use of free solutions for transferring files is very prevalent behind corporate firewalls. Having a centralized way to administer this is a key benefit for IT. The result is that while IT may be charged with archiving or otherwise managing content for legal, regulatory or other purposes; it lacks the ability to fully control the flow of information sent through email. Further, IT has almost no visibility into content that is sent via means other than email, such as overnight packages, USB drives, personal email, etc.

- **Auditing content delivery is difficult or impossible**
  Related to the point above is that performing audits or delivery verification of externally sent content is difficult in many cases. For example, if a user sends a time-sensitive proposal to a waiting recipient through email, usually the only way to verify the delivery of this content is to send another email or call the recipient. Most email systems lack the ability to track completely the flow of content from sender to recipient.

- **Legacy file transport solutions typically are not secure and potentially more expensive**
  Some file transport solutions, such as FTP, are often not a secure alternative to email. Many users will share FTP login credentials, content stored on FTP servers can remain in place for years with no control or policies over when this content should be deleted, unauthorized users can find and view content stored on these servers, and so forth. While FTP can be a useful alternative to email for sending content, very often its lack of security negates any advantages if might offer.

- **Users bump into IT-imposed mailbox- and file-size limits**
  Another important issue with which many organizations contend is the difficulty of managing mailbox-size limits. Osterman Research has found that the majority of mid-sized and large organizations impose these limits in order to achieve a balance between server performance, manageable backup windows and user productivity. The problem, however, is that increasing use of email and larger attachments mean that users bump into these limits fairly often, requiring them to spend time deleting content or filing it away onto file servers or in local archives. Aside from the hit on user productivity, this informal deletion and filing of content increases corporate risk by making discovery of content more difficult, more time-consuming and more costly.

  It is also important to note that even if a sender can have their file-size limit increased for sending files, quite often the recipient cannot receive files that large and so the files still cannot get through.

  A related problem occurs when users run into file-size limits that IT has imposed to prevent enormous file transfers from choking email servers. When faced with these limits, users will often resort to personal Webmail accounts to send these files, resulting in an inability to archive, audit or track this content, not to mention the problems associated with sending potentially sensitive material without encryption. Sometimes users will print the contents of large files or burn a CD or DVD and send the content via overnight courier, driving up costs.

The Benefits of an Attachment Management Solution

To say that email as a file transfer solution is broken would certainly overstate the case. However, there needs to be a better way of sending electronic content in almost all organizations, particularly in cases where users need to send large files. To address the problems discussed above, any organization should seriously consider the use of an attachment management solution. Among the benefits of such a solution are:

- **It offloads content from email servers**
  One of the chief advantages of an attachment management solution is that it bypasses the corporate email system, sending content through an alternate channel. Using the research data discussed above, an attachment management solution that was used for all file transfers would eliminate more than 98% of the traffic that currently flows through email systems. Even if an attachment management solution

were used only for files of larger than five megabytes, more than 40% of email traffic would be eliminated.

The benefits of eliminating this much email traffic are several, including more responsive email servers, faster message delivery times, slower growth in email storage, lower costs for additional infrastructure, lower IT labor costs, shorter backup windows, and faster restores after a system crash. It is also important to note that using a separate file transfer infrastructure can help an organization extract greater value from their existing (and typically significant) investment in their email infrastructure.

- **An easy way to migrate to the cloud**
  A SaaS attachment management solution is a viable and valuable way to minimize disruption in an email infrastructure deployment while leveraging the benefits of SaaS to eliminate the most significant problems in managing email systems. The use of cloud-based attachment management solutions is a significant first step in moving email investment to the cloud with minimal disruption to existing IT services and investment.

- **It encrypts content**
  The vast majority of attachment management solutions currently available encrypt content, ensuring that the risk of inadvertent data loss is minimized. This lowers an organization’s overall risk of a data breach and can result in greater peace-of-mind for decision makers.

- **It provides auditing capabilities**
  An important benefit of most attachment management solutions is that they allow the tracking and auditing of content sent through them. That means that senders can track when their content was received and, in many cases, who opened it and when they did so. This is an important benefit for demonstrating that commitments and other obligations are met.

- **A hosted solution can reduce overall costs**
  A hosted attachment management solution can reduce overall costs since there are no up-front costs for hardware, software and other infrastructure elements. Other benefits include the shift from a capital expenditure model to one based on operating expenditures, potentially resulting in tax and other benefits. Also (but arguably), hosted vendors may be more innovative and offer better customer service because they must continue to win business each month as opposed to winning a one-time sale.

KEY CONSIDERATIONS IN CHOOSING AN ATTACHMENT MANAGEMENT SOLUTION

Osterman Research believes that there are five important considerations in choosing an attachment management solution:

- **Ease of use**
  Any attachment management solution, hosted or on-premise, must be easy for users or they simply will not employ it as part of their daily routine. A solution that imposes a number of extra steps or that does not fit well into existing workflows will simply be ignored by users regardless of the benefits it offers. The key to success for any alternative solution is to offer a tight, seamless and easily managed integration into the email workflow without impacting the way that users work.

- **It must not impose file-size limits**
  It almost goes without saying that an attachment management solution must either not impose file-size limits or these limits must be so high as not to impede the transfer of content. Any attachment management solution that does impose unreasonable file-size limits will simply remain unused, resulting in the same problems that organizations today experience with email as a file transfer tool.

- **Training requirements should be minimal**
  Along with ease of use for an attachment management solution is the requirement that user training is minimized. An attachment management solution that can quickly be learned will be used more broadly and will minimize the cost of switching from email as a file transfer solution to a true attachment management solution.

- **Must allow auditing of content for legal and regulatory requirements**
  An attachment management solution must permit content that it transports to be audited, providing sufficiently detailed reports about message delivery so as to satisfy legal and regulatory requirements.

- **Must integrate with corporate systems and policies**
  An attachment management solution must "fit in" to the existing corporate infrastructure, integrating with the formal and informal workflows and policies that exist in an organization, as well as the existing email, CRM and other key elements of the infrastructure.

About YouSendIt

With more than 18 million registered users in 193 countries, YouSendIt, Inc. is the number-one secure digital file delivery company. Professionals within 92 percent of Fortune 500 companies use YouSendIt to transfer files too large to send via email, eliminating the need for cumbersome FTP sites and expensive overnight couriers. By sending files and attachments through YouSendIt, corporations can alleviate and better manage the acute challenges of ever expanding email inboxes and overages. YouSendIt integrates seamlessly into the most common desktop tools, including Microsoft Outlook, Microsoft Office, Adobe Photoshop, Final Cut Pro, etc. Users can also access the service through the YouSendIt Web site or the YouSendIt Express desktop application. Visit www.yousendit.com or the YouSendIt blog at http://blog.yousendit.com for more information.

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, statue, 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.

[i] Source: unpublished Osterman Research, Inc. survey data

[ii] Source: unpublished Osterman Research, Inc. survey data

[iii] Source: *Results of a Survey on the Use of Email, Social Networking and Other Applications*; Osterman Research, Inc.; published April 2010

[iv] Source: *Results of an End-User Survey on Messaging Issues*; Osterman Research, Inc.; published February 2008

[v] Source: Content Archiving Market Trends, 2010-2013; Osterman Research, Inc.; published July 2010