

**THE TOP 5 REASONS  
WHY YOU SHOULDN'T USE  
EMAIL FOR FILE TRANSFER**

WHITEPAPER

In today's global business environment, email may be the most critical communication tool for a company. Countless messages are fired off worldwide everyday, and while the emails containing just text usually find their destination, things aren't so certain for emails carrying attachments. File-size caps, server hiccups, spam filters—all of these can derail an email as it tries to reach its destination.

**REASON #1:**  
**Email Can't Support Large File Attachments**

**REASON #2:**  
**Updating Email Infrastructure Can Wreck It Budgets**

**REASON #3:**  
**Large Files Mean Slow Systems**

**REASON #4:**  
**Email Systems Aren't Secure Enough For Today's Business Needs**

**REASON #5:**  
**Email Transfer Is Unreliable, Untraceable, and Can't Be Guaranteed**

For the casual home user, the occasional email problem might be acceptable. For business, however, the delivery of time-sensitive files is absolutely critical for both meeting deadlines and maintaining day-to-day operations.

Part of the problem is that it's so easy to attach a file to an email—just point, click, and hit send. Most users don't understand the problems that can occur when sending files as attachments, but IT departments know it well: file-size problems, security issues, lack of tracking and reliability, etc. That's why email issues take up so much time for help desks in companies worldwide.

The need to transfer business files will never go away; in fact, it will only become more critical. What does that mean for the use of email attachments as a primary file-transfer method? If a company wants to ensure safe and timely delivery of critical files, then perhaps it's time to look for an alternative to email for transferring files. Here are the top five reasons why email shouldn't be used for file transfer.

**REASON #1:**  
**Email can't support large file attachments.**

The following scenario has played out in offices around the world countless times. At the end of the day, a dedicated employee finishes a large document or presentation, attaches the file in an email, and hits send. The file whisks away into cyberspace and the relieved employee goes home for the day—only to see a bounce-back email in his inbox the next morning, along with frenetic messages asking where the file is. One company's email server might have a different attachment size limit from the destination server; thus, even though an internal email server will accept a file, it could still bounce back due to target restrictions. That unknown variable can be a great risk to business, especially during crunch time.

Even if they make it through, large files suck up significant storage space in several ways: in the recipient's inbox, in the sender's Sent folder, and in Trash/Deleted folders. This leads to over-quota problems, creating a chain reaction of logistical problems:

- Once an inbox is over quota, it will bounce back any messages sent to it, thus preventing critical communication.
- During this time, frantic IT support calls spike.

- The removal of old messages to free up storage space can result in the deletion of messages/files needed later on. When that happens, more calls are made to IT support.

From bounced-back emails to storage issues, just about everyone in the company is affected when large files are emailed. In the end, this winds up hurting the bottom line and costing staff productivity—something no business can afford to lose.

**REASON #2:**  
**Updating email infrastructure can wreck IT budgets.**

When email becomes the default method for large file transfer, the problems in Reason #1 become inevitable. In order to keep email as the preferred file-transfer method, IT departments can pursue one (or both) of two options:

- 1) The IT department increases its active monitoring of the mail storage server, addressing issues and contacting appropriate employees when problems arise. Because business is a 24/7 global environment today, this requires continuous observation and analysis, pulling valuable resources away from other core tasks for troubleshooting, problem solving, and monitoring.
- 2) The IT department can spend more to upgrade hardware for increased mail storage requirements. However, a complete restructuring of email infrastructure comes with its own budget-busting price tag. The following table is a Year One analysis of hardware/software costs to support a Microsoft Exchange mailbox system:

**HARDWARE/SOFTWARE**

Server Hardware	\$4,000.00
Backup Domain Controller	\$2,000.00
Exchange 2007 Server License	\$699.00
Windows 2003 Server (5 Licenses)	\$999.00

**LICENSING**

Exchange 2007 Server Standard User Licenses	\$67/user
Windows 2003 Server User Licenses	\$40/user
Outlook 2007	\$129/user
Anti-Virus	\$15/user

**BACKUP HARDWARE/SOFTWARE**

Backup Server	\$2,000.00
Backup Exec Software	\$1,000.00

**YEAR-ONE  
HARDWARE/SOFTWARE  
TOTAL: \$10,698**

**YEAR-ONE LICENSING  
TOTAL: \$251/user**

That cost doesn't include other additional security options, such as encryption and notification/tracking.

Any way you look at the numbers, there's no getting around the fact that an entire infrastructure upgrade will be costly. Even when it gets up and running, the problems from Reason #1 will continue to accumulate over time.

**REASON #3:**  
**Large files mean slow systems.**

Picture a three-lane highway with cars and trucks moving along at a fast pace. Now imagine what happens if an oversized truck barrels down the highway, taking up two lanes while flashing emergency lights. The whole freeway slows down; in some areas, traffic will totally stop until the truck passes by. Why? Because the infrastructure can't support something that large without disrupting the regular flow of traffic.

In that scenario, cars and trucks are regular emails and that oversized truck is a large attachment being sent through the email server. Email servers aren't designed to handle large file transfers, and the process of delivering those files slows down network traffic. In a best-case scenario, things temporarily slow down while the large file moves from Inbox A to Inbox B. In a worst-case scenario, the infrastructure can't handle the overload and the email server crashes. Imagine the likelihood and the risk of this happening in medium or large corporations with hundreds if not thousands of users, where mail servers are handling numerous message transactions at any given point in time.

There's a reason why email systems have a cap on file sizes. Simply put, email servers weren't meant to be file-transfer conduits. File-size limits are meant to ensure that the infrastructure never encounters anything it can't handle. These limits can be one of the most frustrating issues facing end users. With files increasing in size as applications become more advanced and complicated, the file-size safeguard becomes a hindrance to day-to-day business users, slowing down communication—or even grinding it to a halt.

**REASON #4:**  
**Email systems aren't secure enough  
for today's business needs.**

When files are attached to emails, they are routed over the public internet in clear text without any encryption. It's similar to carrying confidential

papers in a see-through briefcase; if the wrong people look hard enough, they'll see exactly what you don't want them to see. Can a business trust confidential information (financial records, client information, proprietary designs, etc.) in an unencrypted system? With online security becoming more and more critical every day, company risk and employee liability are very real factors when dealing with private data.

Beyond encryption, other issues demonstrate the need for further security features not provided by standard email systems. With confidential information, it is absolutely imperative that the right person gets the file. Using an email application, this is performed simply by entering in an email address—and when programs auto-fill the wrong sender from an address book, one careless mistake can be devastating to a company's proprietary data.

In a situation like that, how can you actually tell that the email was sent to the wrong person? You could call the intended recipient to check to see if they got it or you could check your Sent folder to verify the address. In other words, no automated tracking and notification process exists for the end-user to control this.

From an IT perspective, this becomes an issue of standardization: how can the IT department centrally control and manage corporate communication when it comes to sending proprietary information? With email, this remains in the hand of the end-user, leaving critical files to the whim of hurried employees under deadline pressure.

Taking a further step back, the needs for encryption and security are starting to come from external sources rather than within the company or IT department itself. Consider the rapid increase in government-sanctioned encryption/security and data privacy requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act of 2002 (SOX), the Gramm-Leach-Bliley Act (GLBA), and various state-level data privacy breach notification

laws. Legislation such as these acknowledge the growing reliance on online communication to expedite business and information sharing; yet at the same time, these acts create rigid standards that must be met by IT departments in their respective industries.

Each year, the size of application files grows bigger and bigger. At the same time, security restrictions increase due to a growing focus on confidentiality and protection. Ultimately, every passing day further antiquates the use of email for large file transfer.

**REASON #5:**  
**Email transfer is unreliable, untraceable, and can't be guaranteed.**

How many times does the question “Did you get my email?” get asked every day? When emails fail to arrive quickly, there could be any number of reasons. Sometimes, the sender can do everything right—obey file-size limitations, enter the proper email address, confirm that they hit the Send button—and the email with the critical attachment still fails to show. Files sent as email attachments can be delayed or blocked due to server issues, the files could mistakenly be considered as a security threat or spam and thus sent into the junk mail folder, or the email may have been simply overlooked by the receiver because of the numerous emails bombarding us every day.

For “snail” mail, the U.S. Postal Service gives you the option to pay extra for notification, tracking, and delivery confirmation. Email systems don't natively come with those options. While some third-party plug-ins exist to confirm delivery, they lack any sort of integration with file attachments. There's simply no way to tell when or if a file was downloaded, whether the download was successful, or when that download occurred. In addition, because email attachments have no tracking system to verify who receives them, proprietary information can be inadvertently exposed.

In fact, the only way to confirm that time-sensitive

proprietary files arrived via email is to call and verify with the recipient. With tight deadlines and tall demands, that level of verification can be a second job unto itself, creating all sorts of drags on productivity and ultimately hurting an organization's bottom line.

## The Next Step In File Transfer

The use of email for file transfer is the proverbial square peg in a round hole: it's forcing the platform to do something that it was not designed to do. What's needed is a platform designed specifically for file transfer—a solution that addresses the limitations of emailing attachments while improving the bottom line and streamlining budgets with minimal hardware upgrades or maintenance.

A dedicated file transfer solution is the logical answer to the aforementioned email-for-file-transfer issues. The next step, then, is to define what makes an ideal file transfer choice. The following are five key things to look for in a file transfer solution:

- 1. Ease of use:** Some file transfer solutions frustrate users with an unfamiliar interface. On the other hand, the best solutions offer simple functionality that mimic email interfaces, or better still, direct integration with email clients such as Microsoft Outlook or Novell GroupWise to offer a seamless user experience.
- 2. Transparency and tracking:** Was your file successfully sent? Was the recipient notified? Who opened it and when? With security compliance and data privacy regulations abound, the ability to know where your documents are in the transfer process is necessary for meeting deadlines and delivering proprietary data. Transparency and tracking are absolutely essential for today's businesses and must be a key component of any good file transfer solution.
- 3. Centralized administrative controls:** For IT departments, nothing slows down efficiency more than having to police individual workstations. A good file transfer solution is

## LeapFILE, Inc.

### Essential Compliance Solutions Secure File Transfer & Collaboration

phone:  
+1 (888) 716-9380  
email:  
sales@leapfile.com  
web:  
www.leapfile.com  
blog:  
http://blog.leapfile.com  
twitter:  
http://twitter.com/leapfile

built for the specific needs of business users (as well as IT administrators) and provides centralized administrative controls for swift single-point deployment and management. Look for capabilities to enforce company-wide usage and security policies as well as integration with active directory servers for large company rollout.

**4. Provider-hosted applications:** When businesses elect to use Software-as-a-Service (SaaS) file transfer solutions, they instantly save time and money. Why? Hosted solutions require no upfront costs or additional hardware resources; instead, IT managers can easily scale service-plan subscriptions based on real-time need. Because all upgrades—both major and minor—are performed on the provider's side, IT departments are free of deployment issues while users always get the latest technology. The best solution providers maintain dedicated account support so that service and help desk requests from users are handled by the vendor rather than by the company's own IT staff.

**5. Reliability:** When shopping for a car, you want a reputable dealer known for service, price, and trust. A file transfer solution is no different; the provider must have a consistent and successful track record of being innovative and reliable when addressing file transfer needs. Good indicators of a reliable solution provider include its list of major clients served (particularly in the same industry or market as the company), service level agreements (SLAs) to guarantee solution uptime/availability, and certifications such as SAS70 Type II to audit for internal controls.

Ease of use, transparency and tracking, centralized administrative controls, provider-hosted applications, and reliability: those five items are the tent poles of the best file transfer solutions. They prop up individual needs while supporting the bigger picture and bottom line—and if one of them is lacking in any way, the value of the entire package could collapse. It's a risk that IT administrators simply can't afford to take. Thus, the

question remains: where can they find an affordable file transfer solution that fulfills those needs?

## Introducing LeapFILE

For IT departments fed up with the limitations and liabilities of email file transfer, LeapFILE represents a secure, effective, and viable SaaS alternative. LeapFILE is a managed file transfer and file collaboration suite built specifically for transferring and sharing files. Available as either a web-based solution or a desktop client (featuring plug-in integration with popular email clients including Outlook and GroupWise), LeapFILE is a fully hosted solution that removes the file transfer burden from local IT departments.

LeapFILE's other benefits include:

- Multi-user accounts deployable with active directory integration
- A support team dedicated to solving LeapFILE user issues
- Fully integrated with popular apps such as Outlook, Office & GroupWise
- Detailed tracking & reporting for auditing purposes
- Full control with IT admin panels for usage & policy enforcement
- Heavy security features such as encryption, SAS70 Type II certified data centers, automatic file expiration settings, etc.

Cost effective, easy to use, easy to integrate, and easy to manage, LeapFILE is the premiere file transfer solution for businesses seeking a stronger and more secure method to transfer large and/or confidential files. Trusted by more than 2,000 businesses worldwide, LeapFILE provides safe and effective file transfer covered by guarantees of 100% network uptime/99.9% application uptime.

**Learn more details or request a personalized demo at [www.leapfile.com](http://www.leapfile.com)**