eWEEK
THE ENTERPRISE NEWSWEEKLY

PREPARED FOR TUMBLEWEED COMMUNICATIONS

The Why, What, and How of Managed File Transfer in Business

EXECUTIVE OVERVIEW: Secure and reliable file transfer is a critical function for many IT organizations. Transferring data efficiently, securely and rapidly to internal and external partners is a skill that's critical to remaining competitive. Now more than ever, IT organizations must closely track file flows, identifying:

- Who is handling files/data
- When files are being exchanged
- To whom(where) data is being exchanged with (source and destination)
- How files are being transferred (FTP, email, securely or nonsecurely)

This paper will examine how organizations like yours are meeting the challenges of finding more secure and reliable ways to manage file transfers. It isn't our goal in this paper to take you into a detailed technical discussion of file transfer; rather we will give you some of the concepts and terms so you can understand the significant technical challenges and solutions. In that way, you'll be more equipped to develop the right solution for your organization.

For this paper, Ziff Davis commissioned a survey on file transfer. We surveyed people in a variety of businesses including a large percentage in finance and healthcare. It isn't surprising that people responding to our survey report wanting highly secure, reliable, and affordable file transfer solutions. But, surprisingly, the survey points out that a large number of organizations are using unsecure methods of transferring sensitive data.

ZIFF DAVIS MEDIA
CUSTOM PUBLISHING

INTRODUCTION: Depending on the line of business, the types of data being exchanged with business partners, customers, constituents, and internal users varies. Often, that data includes highly sensitive information like account data, personal information, intellectual property, or other critical business operations. Just-in-time ordering, supply chain management and speedy fund clearance make file transfers a critical part of modern business processes.

Depending on the types of data the files contain, the file transfer process may be required to comply with specific regulations and laws. Other types of data like personal information and intellectual property contain confidential information that is highly sensitive, but not governed by regulatory mandates. When we survey businesses we often find that the file transfer system in place is unsecured, unmanaged, and vulnerable to random communication problems. These systems are often based on FTP, a protocol with few security features in its native mode.

Improving the way a company transfers files can make a positive impact on the efficiency and profitability of that business while solving problems of security and reliability. Many businesses start using file transfer by attaching PDF or EDI document files to email messages. This technique can work if you only need to transfer a small number of files that are small in size, but it doesn't provide guaranteed delivery, good security, or any management tools. You are flinging files into a dark pool of email along with all of the world's spam and trusting that the files arrive safely. In many organizations, limits on the size of file attachments are imposed on corporate email servers; resulting in failed transmissions and the threat of business data reaching some unknown destination. You don't get the benefits of strong security, reporting or management when you transfer files using email.

The File Transfer Protocol or FTP is part of the TCP/IP family of protocols and it defines how files move between two end points called servers and clients. Programs that conform to the FTP protocol, including browsers and file transfer utilities, typically include menus that make it easy to find the desired destination of the file transfer, to initiate and monitor the transfer, and to report completion of the transfer. But, some FTP implementations send passwords in the clear, don't guarantee that the received file is free of errors, tangle with firewall security, and have rudimentary management reports. With FTP you don't always know what you get.

There are several ways to secure FTP activities, but they present a complex process because of the separate control and data streams involved. Many researchers and organizations have security enhancements for FTP and secure alternatives to FTP. You'll see references to Secure FTP (SFTP), FTP over the Secure Shell (SSH), and Secure Sockets Layer over Transport Layer Security (SSL/TLS) among others. AS3 is a relatively recent standard describing security enhancements for FTP. Some of these protocol systems require an extensive public key security infrastructure. Some of them interoperate but some do not.

The facts about FTP that you need to take away are:

- You must be very careful when you use FTP because adding enhanced security and relability patches can cost you in overhead, interoperability, and flexibility.
- Homegrown "kludge" solutions face many barriers to success and might not comply with government-mandated requirements.
- A true managed file transfer solution will include security, management and reporting/auditing measures as an integrated part of the solution.

Integrated managed file transfer systems use dedicated servers and secure client software. The specialized server offers flexibility, scalability, and dashboard-style management. It overcomes the challenges of different protocols and security schemes while maintaining controls that meet regulatory and legal compliance requirements.

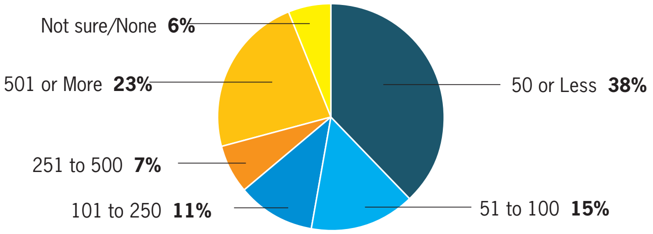
Now, let's see how real people in real companies handle the problems of making secure and reliable file transfers.

THE SURVEY: Ziff Davis commissioned a study that gained complete responses from 1,159 people who are involved in or familiar with file transfer solutions used within their organizations. The Strategy Group, an independent research company located in Englewood, Fl, conducted the study. The largest business sectors represented in the survey were non-computer manufacturing, finance and banking, and healthcare/medical.

VOLUMES: To get an idea of the volumes of data, we asked how many external end users are involved in file exchanges. Almost a quarter of the respondents say that they were exchanging files with more than 500 external destinations. (Figure 1)

Over a third of these companies reported moving more than 50 gigabytes of file data a week and 11% reported moving more than 700 gigabytes a week. A large number of companies, 21%, reported exchanging more than 2,500 files per week.

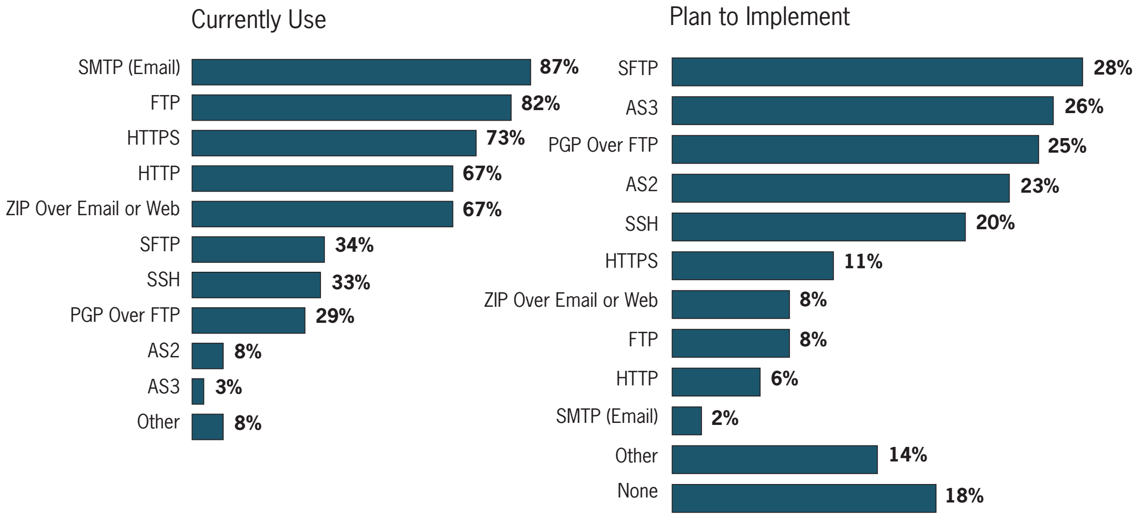
(Figure 1) NUMBER OF EXTERNAL END USERS COMPANY EXCHANGES FILES WITH:
Average number of end users: 247
Q. How many *external end users* does your company exchange files with?



THE ROLE OF EMAIL: Right now, many of the people in our study use email as some part of a file transfer solution. (Figure 2) The clear trend is to get away from email and into some form of secure FTP. But, as we explained earlier, not all secure FTP is the same and interoperability can become the next problem to be solved.

The people responding to this survey tell us that email is not a practical way for the majority of companies to exchange files. They need a process able to handle the volume of data and the variety of destinations in a secure automated manner.

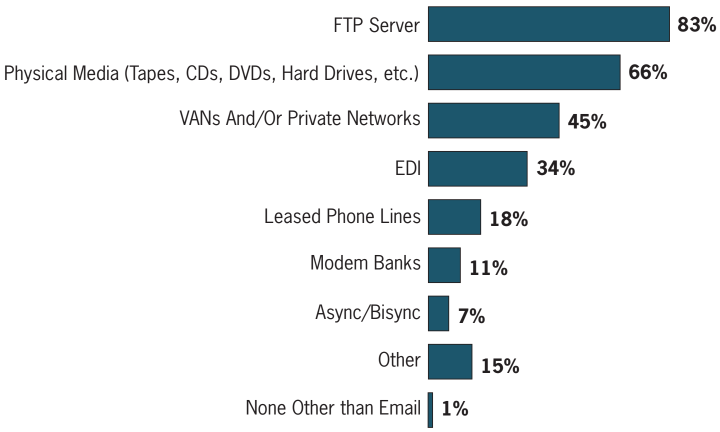
(Figure 2) INTERNET FILE TRANSFER PROTOCOL CURRENTLY/PLAN TO USE
Q. Which Internet file transfer protocols do you use today?
Q. Which do you plan to implement during the next 12 months?



WHAT ARE COMPANIES DOING? An interesting finding from the study is the number of companies using physical media to transfer information. (Figure 3) It is true that couriers and express companies have great bandwidth. Sending tapes, CDs, and other media by express delivery can move a lot of data. But, in addition to the vulnerability of lost or stolen data, in today's markets that data is out of date before it arrives. International commerce doesn't wait for distance barriers and moving any package quickly over a long distance is expensive. Secure and reliable managed file transfer systems can provide the timeliness that is missing from media transfers.

(Figure 3) MECHANISMS COMPANY USES TO EXCHANGE DATA AND FILES

Q. Besides Email, what mechanism(s) does your company use to exchange data and/or files with customers, suppliers and/or business partners?

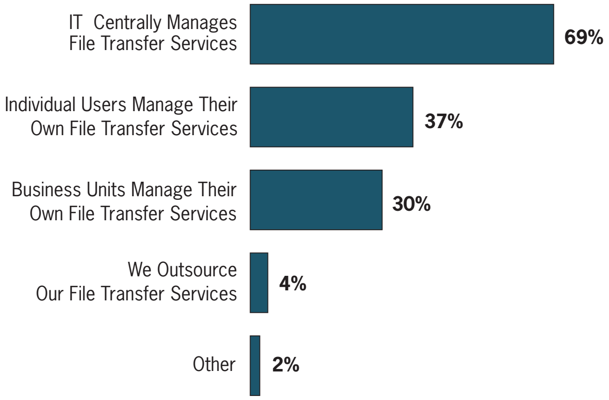


WHO IS WATCHING THE PROCESS? Who manages this critical business operation? As the chart below shows, there is an important sharing of responsibility between IT and individual users. This fits in with the trend of "IT as a Service" that currently is the subject of so much comment and analysis.

Our survey tells us that IT delivers the service, but that it is often individual users (Figure 4) and business units that use the service. A good file transfer system has centralized management and decentralized execution.

(Figure 4) HOW FILE TRANSFER IS MANAGED

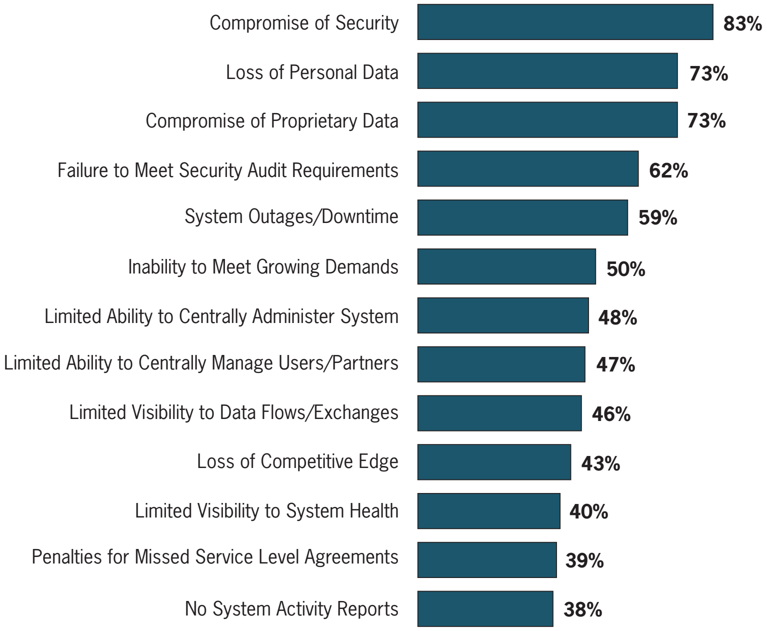
Q. How is file transfer managed in your organization?



BUSINESS NEEDS: It comes as no surprise that our survey respondents want the "-ilities". (Figure5) In addition to security, they want reliability, affordability, and manageability that comes with a well designed managed file transfer system. The emphasis on management came through clearly. (Figure 6) It is extremely unlikely, if not impossible, that the people in our study can meet their expressed needs for security, reliability, affordability, and manageability using "home grown" file transfer solutions.

(Figure 5) COMPANY'S CONCERNS ABOUT TRANSFERRING FILES (PERCENT OF RESPONDENTS CITING CONCERNS BY SELECTING 4 OR 5 ON A FIVE-POINT SCALE)

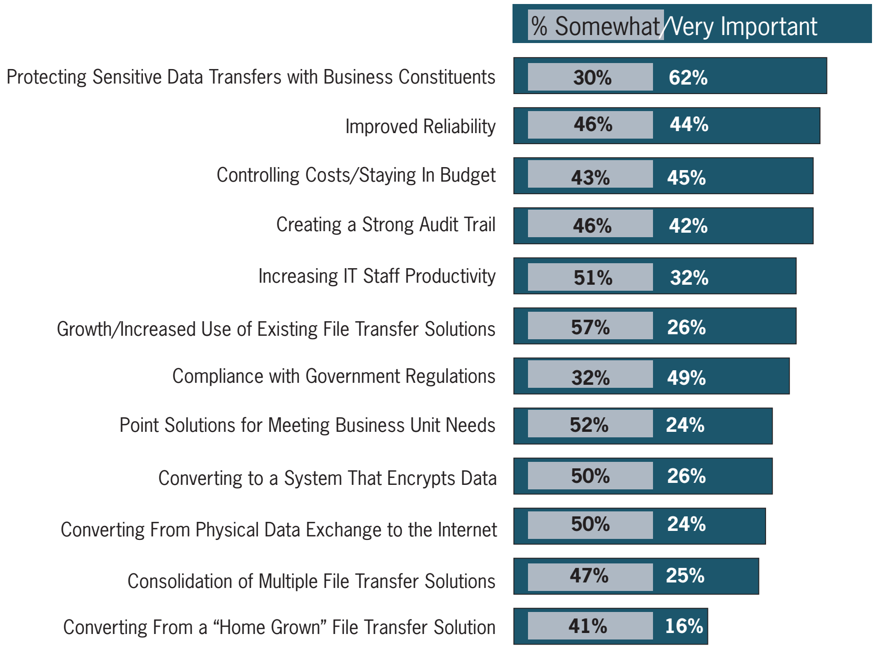
Q. Using a scale of 1 to 5, where 5 means "Very Concerned," and 1 means "Not Concerned At All," what concerns your company most about transferring files?



(Figure 6)

IMPORTANT BENEFITS OF FILE TRANSFER CAPABILITIES

Q. How important are each of the following benefits in driving your investment, or continuing investment, in improved file transfer capability in your organization?



THE FEATURES BUSINESS PEOPLE NEED: We asked our survey group to rank the features that are important to them in a business-to-business file transfer system. (Figure 7) Encryption, authentication, and file integrity scored high. Forty-five percent of the respondents encrypt specific categories of files such as financial and personnel records. Forty-three percent encrypt all data during transmission. Encryption by category leaves room for error and transmission without encryption is playing roulette.

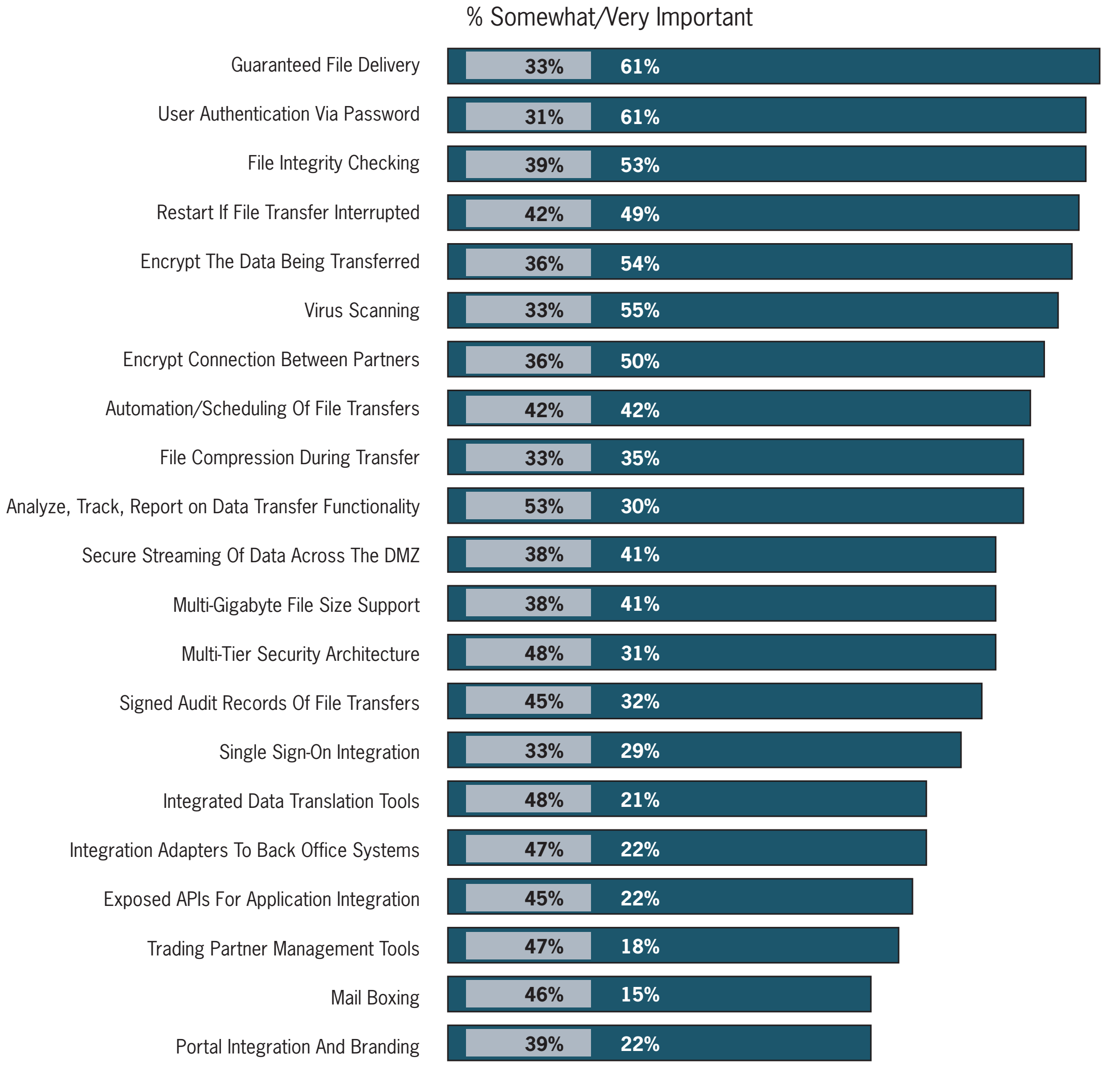
Analysis, audits, and reports were nearly as important as the technical side. It's good to move the files efficiently, but you must be able to prove and improve the actions.

SUMMARY: Whether your company transfers files with 10 users or more than 500, each transfer carries with it the risk of sensitive data falling into the wrong hands, a failed transfer or a breach of security policies or regulatory guidelines. Managers need a clear understanding of the types of information being exchanged and the associated requirements for sensitivity and confidentiality. A true managed file transfer solution will include security measures as an integrated part of the solution. While security measures may add some overhead, the reduced risk that results will make the investment worthwhile.

(Figure 7)

IMPORTANCE OF B2B FILE TRANSFER FEATURES

Q. Please rate the importance of the following business-to-business file transfer features to you.



MANAGED FILE TRANSFER SOLUTIONS:

With managed file transfer systems, like SecureTransport from Tumbleweed Communications, organizations can:

- Reduce security risk and management burden by consolidating homegrown FTP server solutions
- Replace disparate and expensive legacy mechanisms such as leased lines, VPNs, or modem pools
- Automate and streamline applications and processes requiring file transfer
- Manage a large trading community
- Securely transfer sensitive data in compliance with industry and government regulations
- Conduct B2B and EDI transactions securely and reliably using standards-based Internet protocols with FTP, secure FTP, HTTP, HTTPS, SSH (SFTP and SCP) and AS2
- Audit and report on data exchanges prove compliance