

## EVOLUTION FROM FTP TO SECURE FILE TRANSFER

### DAVID STELZL, CISSP

Preeminent expert on digital asset protection strategies, an information security professional who inspires audiences and readers by showing them how to look at security, digital assets, and the protection of mission-critical data.

### SPONSORED BY IPSWITCH FILE TRANSFER

### ABSTRACT

Do you know where your organization's confidential and sensitive files were transferred today? Are you sure they even made it to the right people and not into the wrong hands? Are you concerned with the information and data sharing practices in your company? If so, you are not alone.

Lessons learned from recent high visibility data breaches illustrate how the combination of not following sensible file transfer best practices coupled with improper controls over the file transfer environment can and has been a part of company-ending events. As a result, more and more organizations are moving away from basic FTP solutions and quickly moving towards information exchange solutions that incorporate secure file transfer.

This paper will discuss how secure, reliable, and Web-based file transfers can help your organization achieve its key business goals while reducing the amount of organizational distraction caused by not having a well understood and managed file transfer process that is aligned and integrated with your core business processes.

## EVOLUTION FROM FTP TO SECURE FILE TRANSFER

### **What is at stake:**

Trust of your business partners • Loyalty of your customers • Efficiency of your business

### THE IMPORTANCE OF YOUR FILE TRANSFER SOLUTION

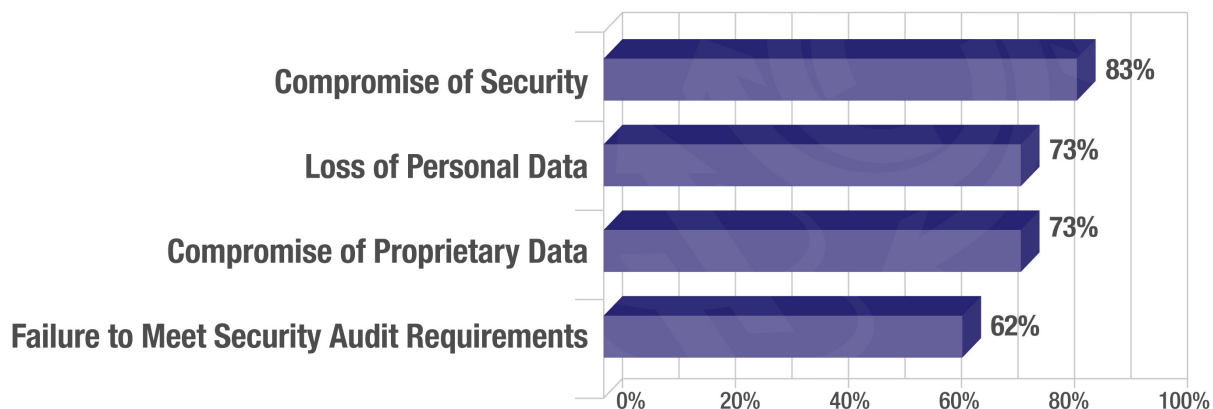
Customers, remote employees, and business partners have to exchange critical data over the Internet. It's no longer just a convenience – effective file transfer is often key to the way organizations run their business and their overall competitive advantage.

However, many companies today are challenged with finding more secure, efficient and reliable ways to manage file transfers. Electronically exchanging company information — such as financial data, client data, health records, employee data and other intellectual property — carries with it the risk of sensitive data falling into the wrong hands or not even making it into the right hands.

It's a significant risk. Failure to adequately protect your data can lead to productivity loss, fines for non-compliance, a tarnished public image, and the long-term trust and loyalty of your partners and customers. All of this is dependent on the strategic and tactical implementation of your file transfer processes.

Are you concerned with file transfer practices in your company? If so, you're certainly not alone. According to a research report from Ziff Davis, the overwhelming majority of survey respondents who are familiar with the file transfer solutions used within their organizations feel the same way.

### WHAT ARE YOUR FOUR GREATEST FILE TRANSFER CONCERNS?



### THE PROBLEM WITH BASIC FTP SOLUTIONS

File Transfer Protocol (FTP) is often deployed as a simple solution to enable the electronic exchange of business information and data. The adoption of transferring files across the open Internet has been so universally widespread that businesses now consider this ability to be critical to everyday business operations. In fact, it's now estimated that 83% of businesses are using FTP to move and share files and data.<sup>1</sup>

Basic FTP can be a practical and viable method to transfer files if the data being transported is not critical, has no requirement for security and is not considered high risk. However, basic FTP itself is a weak link in the

<sup>1</sup> "The Why, What, and How of Managed File Transfer in Business", Ziff Davis Publishing, 2007.

process of transferring confidential data due to its inherent lack of security and data management.

The business process of file transfer has a history of not being treated as a core part of IT infrastructure or critical to business operations. The management and security of data transfers has often been left to individual contributors and lower-level IT staff. As a result, decisions have often been made from a limited viewpoint to solve individual tasks rather than from a more holistic view of the larger and strategic company need. File transfer solutions have often been relegated to the darkest corner of the lowest wattage server room, and it's very common to find long-ago deployed home grown FTP solutions that are not well understood, documented or easily maintained by today's IT staff being used to manage company data.

The combination of businesses having undervalued high risk data and basic FTP itself being a weak link in the file transfer process presents a huge business liability. Today's evolving regulatory compliance and corporate governance requirements — not to mention the recent onslaught of highly visible data theft incidents — have highlighted the need for something better and more secure than basic FTP.

## BASIC FTP – NOT SECURE, NOT COMPLIANT

The original specification of the FTP protocol included minimal, if any, security. As FTP protocol use has increased and the Internet has evolved and become more and more open, the security limitations of FTP have been exposed. For example, the standard FTP specification does not include the use of strong authentication, such as encrypted passwords or authentication tokens. Sending the login credentials in clear text allows cyber-thieves to sniff login information, which can then be used to gain unauthorized access to data. Even worse, the standard FTP does not encrypt the connection that files and data are being transferred over or even encrypt the files being transferred. Unencrypted file transfer, which can potentially allow a man-in-the-middle attack<sup>4</sup> and unauthorized viewing of data either during transmission or in storage on the server, has become a huge privacy concern today.

Regulatory compliance is another challenge that many companies are now faced with. In order to meet the legal requirements of compliance mandates, corporate governance requirements, and other regulations, data must be managed throughout the file transfer business process. Businesses must sufficiently protect information from harm, whether health or financial records, customer accounts, or intellectual property. Audit trails which prove the safe management and secure movement of information are now a requirement to provide auditors. In such environments, standard FTP is not enough, due to its lack of strong security, data management, monitoring, and process control.

### Improper control of file transfer environment played part in company ending event.

"In September 2004, an unauthorized party placed a script ... on the CardSystems platform ... This script ran on our system and caused records to be extracted, zipped into a file, and exported to an FTP site ..."<sup>2</sup>

"In September 2004, hackers dropped a malicious script on the CardSystems application platform, injecting it via the Web application that customers use to access account information. The script, programmed to run every four days, extracted records, zipped them and exported them to an FTP site.... lesson learned too late for old CardSystems"<sup>3</sup>

- STATEMENT OF JOHN M. PERRY  
(former) PRESIDENT AND CEO  
CARDSYSTEMS SOLUTIONS, INC.  
(now defunct) BEFORE THE UNITED  
STATES HOUSE OF REPRESENTATIVES  
SUBCOMMITTEE ON OVERSIGHT AND  
INVESTIGATIONS OF THE COMMITTEE  
ON FINANCIAL SERVICES HEARING  
ON "CREDIT CARD DATA PROCESSING:  
HOW SECURE IS IT?" WASHINGTON,  
D.C. JULY 21, 2005

### Market drivers for electronic secure file transfer

- Security
- Compliance Regulations
- Corporate Governance

<sup>2</sup> Mimoso, Michael, "Cleaning up after a data attack: CardSystems' Joe Christensen," Information Security News, April 2006, Available online: [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci1180411,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1180411,00.html).

<sup>3</sup> "Hearing on Credit Card Data Processing: How secure is it?", US Committee on Financial Services, Congressman Barney Frank, chairman, July 2005, Available online: <http://financialservices.house.gov/media/pdf/072105jmp.pdf>.

<sup>4</sup> "IT Security Dictionary", IT Security, Available online, <http://www.itsecurity.com/security.htm?s=515>.

## IMPROVE SECURITY – AND FILE TRANSFER SUCCESS

Two common security protocols that help secure and increase the reliability of data transfer, Secure Sockets Layer (SSL) and Secure Shell (SSH), are specifically designed to encrypt file transfers and associated administration network traffic. Both SSL and SSH enhance the security and reliability of file transfer by using encryption to protect against unauthorized viewing and modification of high risk data during transmission across open networks such as the Internet.

### SSL – A SECURE ENHANCEMENT TO STANDARD FTP

If you use a web browser, chances are you have already been using a flavor of SSL encryption, as it was originally developed and has since been widely deployed to protect connections to web servers. SSL, also known as FTPS or “Secure FTP over SSL” is also used in conjunction with FTP to provide secure encryption over standard FTP connections. It uses the same two ports as a standard FTP connection, with the enhancement of the data channel being encrypted. SSL connections encrypt and decrypt FTP sessions across networks to provide authentication of credentials and to secure private communications. There are different strengths of SSL available, the most recent being SSL v3 and TLS 1.0, which are stronger than previous versions.

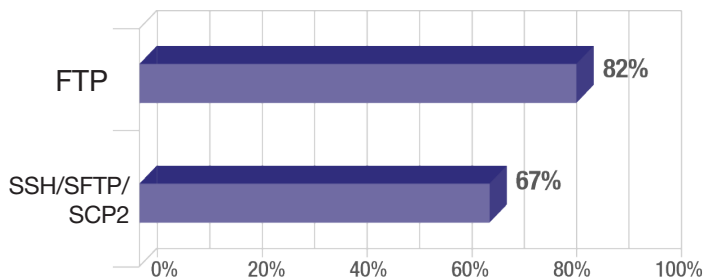
Not only does SSL encryption ensure that the wrong eyes do not gain access to your data, but it also protects against attempts to modify data while in transit. If an attacker could modify your data during transmission, you could not rely on the accuracy of the data when used in your application. SSL connections provide substantially increased reliability and decreased risk when transporting files and data, due to the built-in protection from unauthorized viewing and modification of data during transmission. When using SSL to protect data on your file transfer server, you must also ensure that all connecting file transfer clients support the same SSL capability, as the security must be deployed at both ends of the data transport for it to be utilized.

### SSH – THE PREMIUM CHOICE FOR SECURE FILE TRANSFER

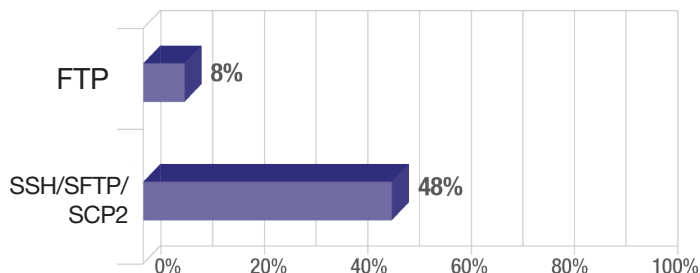
SSH, also known as SFTP or “Secure Shell File Transfer Protocol” is a premium security protocol that delivers secure communications and is often considered the best option for secure file transfer. SSH is widely deployed on various operating systems. It uses Secure Shell 2 (SSH2), a secure tunneling protocol, to emulate an FTP connection and provides a firewall friendly and encrypted channel for file transfers using the well-known TCP port 22. SSH offers enhanced security by having the entire file transfer session, including all session control commands, entirely encrypted at all times while only requiring a single port be opened on your firewall versus the two ports that need to be opened for FTP and SSL connections. Another widely used feature of SSH is Secure Copy (SCP2). It provides interoperability across multiple operating systems, platforms and includes desktops, servers and mainframes.

According to the previously mentioned Ziff Davis report, more and more organizations are moving away from basic FTP solutions and quickly moving towards Secure File Transfer using SFTP.

**FILE TRANSFER PROTOCOLS USED TODAY**



**PLANNED IMPLEMENTATION IN NEXT 12 MONTHS**



The authentication of both SSL and SSH connections can be based on passwords or certificates. If using passwords, they should be of sufficient strength so that they are hard to guess by attackers. Policy-based enforcement of strong cryptography algorithms (and passwords) and being able to control length of encryption keys will protect against unauthorized viewing of data. Such control should be enforced in compliance with your security policy.

SSH is particularly popular in IT environments because most operating systems (including UNIX/Linux) support SSH, therefore using SSH for file transfer (SFTP) allows for cross-platform IT standardization. Standardization using SFTP ensures consistent, strong security policy enforcement and simpler administration. SFTP is very firewall-friendly because it uses a single connection for uploading and downloading, and it improves on the security of standard FTP by encrypting all data transfer traffic, connection control data and passwords to eliminate eavesdropping, connection hijacking, and other attacks. As an added feature, it also compresses all data during the transmission, which can result in faster file transfers.

## SSH/SSL COMPARISON CHART

	Protocol Comparison		
	FTP	FTPS/SSL	SFTP/SSH
<b>PRODUCTS</b>			
WS_FTP Professional -- File Transfer Client	✓	✓	✓
WS_FTP Server with SSH -- File Transfer Server	✓	✓	✓
<b>SECURITY CHARACTERISTICS</b>			
Credential Encryption	✓	✓	✓
Transport Encryption (i.e.: "Data-in-Transit")		✓	✓
FIPS 140-2 Validated Cryptography		✓	✓
Method for Security		<b>Certificate</b>	<b>Keys</b>
Supports PGP File Encryption (ie: "Data-at-Rest")	<b>Optional</b>	<b>Optional</b>	<b>Optional</b>
Supports File Integrity Checking	✓	✓	✓
Built-in Compression			✓
Secure Copy (SCP2)			✓
Number of Ports for Connection	<b>2</b>	<b>2</b>	<b>1</b>

## RECOMMENDATIONS FOR SECURE FILE TRANSFER

Millions of files are electronically exchanged every day. Unmanaged, insecure file transfers present a significant risk to your organization. The best electronic file transfer solution should enable secure, reliable file transfer by providing integrated, strong security of SSL and SSH encryption, along with the tools to effectively manage the end-to-end file transfer process. Worrying about security of breaches during file transfers can be a distraction from your core business. Yet such concern is well founded: if your data is not protected adequately, your relationships with customers, your competitive edge, and even the business itself are all threatened. A reliable and secure file transfer process can ensure that your organization can concentrate on its core business.

To improve the security of your file transfer process, consider the following steps:

- **Treat file transfer as a core business process:** Do a full inventory of your file transfer requirements and have a CxO sponsor. Then move to document, standardize, optimize and fully manage the file transfer activities of your organization. While technology can help in meeting these criteria, businesses must ensure that their file transfer architecture maps to a well thought out and well managed business process.
- **Require secure communications:** Limit all file transfers of sensitive data to SSL or SSH protocol. Do not allow confidential or critical information to be transported by the insecure FTP protocol. Best practices include requiring the use of strong authentication (mutual authentication preferred), granular access control, secure audit logging of all activity, and that file transfer clients connect over the strongest encryption strengths, such as 256-AES encryption over SSH and TLS 1.0 connections, all of which are included in the WS\_FTP solution.
- **Select and standardize on your secure file transfer solution:** An end-to-end solution must incorporate all end users who transfer files with company servers. Both the servers and all connecting clients must support the required security features – remember, your solution is only as strong as the weakest point. Provide a license of your chosen file transfer client to all employees, vendors, contractors and customers who exchange information with your file transfer server. This best practice will ensure that everyone who accesses your file transfer server is equipped with the same level of security, and enable you to leverage economies of scale benefits for user licensing, training and support.

## ABOUT THE AUTHOR

David Stelzl, CISSP, a preeminent expert on digital asset protection strategies, is a dynamic speaker and information security professional who inspires audiences and readers by showing them how to look at security, digital assets, and the protection of mission-critical data. David has spoken to audiences internationally, bringing life to the concepts of information security, systems, networks, and relevant IT/Business solutions. David teaches organizations how to create relevant security solutions that stop the daily attacks against corporate data.

Over the past twenty years David has worked for companies such as Bank of America (Formally NationsBank), McNeil Consumer Products, and a number of regional and global consulting firms. Most recently David developed and managed the Security Practice for Dimension Data, North America PLC. Serving as Director of Security he developed security assessment methodologies, solutions marketing programs, and served on the Global Security council as a strategist, keeping up with security trends, global threats, and regulatory compliance issues in the areas of GLBA, HIPAA, and SOX. David is CISSP certified and has presented topics on security to audiences in the US, Canada, Europe, and Africa.

## ABOUT IPSWITCH FILE TRANSFER

Ipswitch File Transfer division develops and markets a wide range of managed file transfer solutions. Ipswitch brands, MOVEit®, and WS\_FTP® deliver industry leading secure and managed file transfer solutions to over 40 million users. For product and sales information, write to FTsalesNA@ipswitch.com. Visit [www.IpswitchFT.com](http://www.IpswitchFT.com) for more information on the Ipswitch File Transfer division and its range of solutions.



Contact Ipswitch's File Transfer Division