



Understanding the Impact an FTP Data Breach Can Have on Your Business

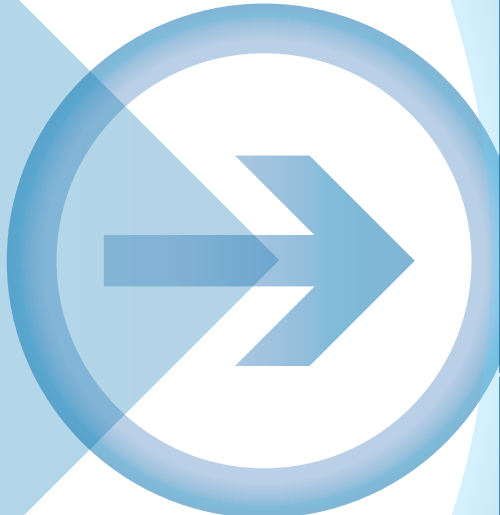


TABLE OF CONTENTS

1	INTRODUCTION	3
2	MAJOR DATA LOSS INCIDENTS OCCUR DAILY WITH DISASTROUS AND COSTLY RESULTS	4
3	FTP: THE ACHILLES HEEL	4
4	FTP: INHERENTLY NON-SECURE	6
5	THE ALTERNATIVES	7
6	REFERENCES	8
7	ABOUT TIBCO	8

Abstract: *With more and more high profile data breaches being reported every day, organizations are being forced to take stock of how they secure and integrate data. Few business events can damage your relationship with customers or derail your business success as drastically as a major data breach. Companies must consider how they may be at risk, and implement best practices to mitigate danger. TIBCO Brief looks at recent data breaches, identifying common points of corporate exposure and ways to eliminate risk.*

1. Introduction

In a recent information security survey¹ conducted by Information Week, only one-third of U.S. survey respondents cited “preventing breaches” as their biggest security challenge. At the same time, two-thirds of the respondents indicated that they feel at least as vulnerable to security attacks as they did last year. Why aren’t companies significantly more worried about lost or stolen company and customer data?

IT organizations often focus significant resources to combat viruses or worms, spyware or malware, and spam. While these problems can cause major disruptions to your network, infect or corrupt files, and negatively exploit your systems in other ways, none can potentially damage your company’s business success and harm your relationship with customers as drastically as a major data breach. While minimizing the effect of viruses or worms, spyware or malware, and spam can reduce your headaches, ignoring open ports on FTP servers can easily result in hemorrhaging from your company’s vital systems – even resulting in irreparable harm to your market position.

2. Major data loss incidents occur daily with disastrous and costly results

- In a highly publicized situation, retailer TJX may be facing anywhere from \$500 million to nearly \$1 billion in expenses as a result of a data breach.² Over 45 million credit and debit card numbers were downloaded by identity thieves..
- A Ponemon Institute benchmark survey³ examined the costs incurred by 35 companies that experienced a data breach and lost protected personal information. Breaches included in this survey came from 15 industry sectors and ranged from less than 4000 to more than 125,000 records. The survey found that costs averaged more than \$6.3 million per breach, ranging from \$225,000 to almost \$35 million.
- A U.S. Department of Justice study⁴ determined that the average loss per incident of data breach was \$1.5 million.

Compounding this variance in the determination of the cost of a breach, a recent Forrester survey⁵ indicated that 25% of respondents did not know, or did not know how to determine, the cost of data security breaches. What does seem clear is that there is a very significant, and sometimes devastating, cost incurred from a data breach.

3. FTP: The Achilles Heel

If your organization uses FTP (File Transfer Protocol) to transfer data from one computer to another, you are at real risk of a data breach and losing critical customer and company information. Why does FTP have the potential to be so dangerous? FTP can be used extensively in business, with little oversight involved, and as a result it can literally be taken for granted. It can easily become subject to carelessness. For example, sharing information with a business partner via FTP makes it vulnerable to data breach. Someone in another department in your organization could bring up an FTP server making data on that system vulnerable. The worse part of these scenarios is that you may not even be aware that an intrusion has occurred! FTP file exchanges pose a tremendous risk of data breach and intrusion by hackers.

How real is this risk? The Associated Press recently obtained detailed schematics of a military detainee holding facility in southern Iraq, geographical surveys and aerial photographs of two military airfields outside Baghdad, and plans for a new fuel farm at Bagram Air Base in Afghanistan. They were able to download this “need-to-know” information in several sessions; the data had been posted carelessly to FTP file servers by government agencies and contractors.

Mike Baker, Associated Press writer, wrote⁶ “The posting of private material on publicly available FTP servers is a familiar problem to security experts hired by companies to secure and police the actions of employees who aren’t always tech-savvy. They [security experts] said files that never should appear online are often left unprotected by inexperienced or careless users who don’t know better.” Mr. Baker went on to say, “File transfer protocol is a relatively old technology that makes files available on the Internet [or a network]. It remains popular for its simplicity, efficiency and low cost.”

This information obtained by the AP is sensitive and could pose a direct threat to U.S. troops. But what about the threat information contained on an unsecured FTP server could pose to a business like yours? Consider a few other recent FTP exposures:

- **CardSystems**, who processed credit card transactions for nearly 120,000 merchants totaling more than \$18 billion annually, were essentially forced out of business after 40 million identities were exposed. **Amex** and **Visa** told CardSystems that they would no longer do business with the company.
- 54,000 records were stolen from **Newcastle City Council**.
- An unsecured document was exposed on the **New Mexico Administrative Office of the Courts** FTP server; it contained names, birth dates, SSNs, home addresses and other personal information of judicial branch employees.
- The Hacker Webzine reports that **Fox News** had an exposed FTP connection linking out to **Ziff Davis**.
- The personal information of uniformed service members and their family members were exposed on an FTP server while being processed by major **Department of Defense (DoD)** contractor **SAIC**. As many as 867,000 individuals may have been affected.

4. FTP: Inherently Non-Secure

FTP is a protocol to easily transfer files on another computer over any network that supports the TCP/IP protocol, such as the Internet or an intranet. Two computers are involved in an FTP transfer: the FTP server, running FTP server software, and a client, running FTP client software. The client computer initiates the connection to the server, and once connected it uploads files to the server or downloads files from the server. The FTP protocol also allows files to be transferred directly from one FTP server to another FTP server.

The original FTP protocol is an inherently easy, but insecure way to transfer files. It contains a number of mechanisms that can be exploited to compromise security. The FTP specification allows a client to instruct a server to send files to a third computer. Known as proxy FTP, this feature causes a well-known security problem as a server can be instructed to send data to a port of a third computer never intended to receive the transfer. There is no provision for encrypting data during transfer. Passwords

and files are transferred in clear text and can be easily accessed. In addition, the specification permits an unlimited number of attempts to enter a password, facilitating password guessing attacks on the system.

Because the FTP protocol is an open standard, it is fairly easy to create FTP server or client software. Most computer platforms support the FTP protocol, so any computer connected to a TCP/IP based network can manipulate files on another computer that permits FTP access on that network virtually regardless of the operating system used. It can also manipulate files on the server by renaming them or even deleting them. The FTP protocol uses two channels: a control channel and a data channel. The connection method can be either active or passive. When using active mode, the client specifies how the transfer is done by choosing a local port and telling the server to send data to that port. The server initiates a connection from port 20 and sends data to the port specified by the client. Firewalls must allow incoming connections to port 20, and hackers can scan the server by initiating connections from port 20.

In passive mode, the FTP server opens a random port and sends the client the server's IP address to which to connect. The server chooses a port that has been incremented by one from the last new connection. The server then waits for the connection from the FTP client. Since the client initiates the connection, it is not

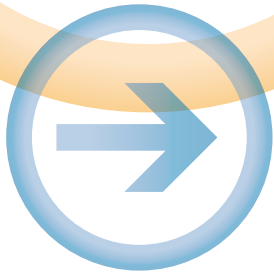
necessary to put holes in the firewall to facilitate incoming connections. Because the server waits for the client to connect after it has opened a port, a hacker has the opportunity to connect instead of the intended user and gain access to the files.

FTP is not a good method to transfer files when authentication is required or when the data is sensitive in nature. If a file transfer is interrupted, the receiver of the transfer has no way to determine if they have received the entire file. Basically, FTP is an unreliable way to conduct critical business communications. Its ease of operation comes with a huge risk and potential cost from data breaches, attacks by hackers and disgruntled employees, and lack of security compliance. Companies utilizing FTP protocol for data transfer aren't even always aware of the amount of unsecured activity that is going on. Are some of your company's information assets sitting out in a network on an unsecured FTP server or an unsecured FTP server of a business partner? In these instances, you will probably never know what's happening with your data. Ignorance, in this case, is not bliss.

5. The Alternatives

There are ways to secure FTP servers, such as FTP over SSH or SSL protocol. These solutions address security by providing encryption on messages between the client and the server, but do not provide automation, management, and control of the file transfer process. In addition, they often require complicated scripting, presenting a drain on an organization's IT resources.

If you need to transfer files other than just public downloads, a managed file transfer (MFT) solution will provide you total control and visibility of your file-based business processes, with every business process documented, auditable, and accountable. MFT is now a strategic necessity, the linchpin to an overall business information strategy within your company and between your business partners. An integrated MFT solution lets an organization impose security and control over all the enterprise's file-based processes. It is an imperative for any organization to be able to get data to the right place, at the right time, in the right format, with guaranteed delivery – while ensuring its security at every step. A leading analyst firm notes that a managed file transfer deployment should be part of an overall integration strategy. Managed file transfer is a critical infrastructure decision, one that you should have to make only once when you implement the correct solution to support your business objectives.



6. REFERENCES:

1. Larry Greenemeir, "IT Security: The Data Theft Time Bomb," InformationWeek, July 14, 2007
2. Andy Patrizio, "How TJX Became a Lesson in Proper Security," Enterprise, December 5, 2007
3. Ponemon Institute, LLC, "2007 Annual Study: U.S. Cost of a Data Breach," November 2007 (Sponsored by Vontu, Inc. and PGP Corporation)
4. Trusted Strategies, L.L.C., "Network Attacks: Analysis of Department of Justice Prosecutions 1999 – 2006," August 28, 2006 (Commissioned by Phoenix Technologies, Ltd.)
5. Khalid Kark, "Calculating The Cost Of a Security Breach," Forrester Research, Inc., April 10, 2007
6. Mike Baker, "Military Files Left Unprotected Online," Associated Press, July 12, 2007

7. About TIBCO

TIBCO Software Inc. (NASDAQ: TIBX) is a provider of infrastructure software for companies to use on-premise or as part of cloud computing environments. Whether it's efficient claims or trade processing, cross-selling products based on real time customer behavior, or averting a crisis before it happens, TIBCO provides companies the two-second advantage™ - the ability to capture the right information, at the right time, and act on it preemptively for a competitive advantage. More than 4,000 customers worldwide rely on TIBCO to manage information, decisions, processes and applications in real time. Learn more at www.tibco.com.

TIBCO® Managed File Transfer Suite

TIBCO MFT connects people, processes and information, thereby promoting and strengthening the value chain among your partners, customers, and employees – both inside and outside of the enterprise.



Global Headquarters
3303 Hillview Avenue
Palo Alto, CA 94304

Tel: +1 650-846-1000
+1 800-420-8450
Fax: +1 650-846-1005

www.tibco.com