

# Peer to Peer

## Risky Business



Peer to Peer March 2010

# A Data Breach Pandemic

BILL HO BISCOM

**T**he frequency of data breaches has accelerated in the last few years as businesses continue to expand globally, increase interactions with partners, suppliers and business associates, and collect and store more data about their customers and clients.

A number of major security breaches regarding personal records have made headlines over the past decade. The following examples comprise only a very small number of the nearly 350 million sensitive records that have been involved in data breaches from 2005 through 2009.

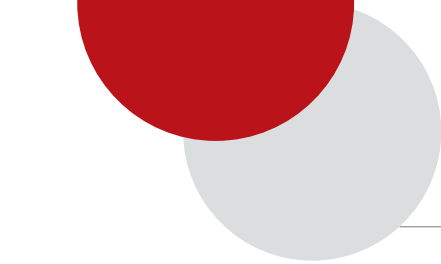
- For eight days in May 2006, an unsecured document was exposed on the FTP site of the New Mexico Administrative Office of the Courts. Exposed data included the names, birthdates, social security numbers and home addresses of 1,500 employees.
- An employee with the National Finance Center mistakenly sent an Excel spreadsheet containing Commerce Department employees' personal information to a co-worker via e-mail in an unencrypted form in August 2009. The names and social security numbers of at least 27,000 employees were exposed.
- In October 2007, a computer tape containing the full

names, addresses, phone numbers, social security numbers and marital status of 200,000 members of the West Virginia Public Employees Insurance Agency was lost while being shipped via United Parcel Service.

The response from federal and state authorities to these breaches has been a growing body of regulations mandating that confidential and personally identifiable data be protected from data breaches both at rest and in transit. Law firms face increasing regulatory compliance challenges around the transfer of confidential client data over unsecure public networks. Typical methods for transferring documents and files to external parties — including FTP, unsecure e-mail and delivery via courier services — can result in data breaches that can expose a law firm to significant financial liability and can negatively impact a firm's reputation. As a result, law firms are reassessing their current file transfer practices and are looking for more secure alternatives.

### DATA BREACH REGULATIONS

Federal data privacy regulations targeting industries such as financial services, healthcare and legal have been in place for several years. Law firms representing clients in these industries may be forced to comply with these regulations as they relate to protecting their clients' confidential data. Examples include payment card industry standards to protect credit card



holder information and the Gramm-Leach-Bliley Act's Safeguards Rule that requires financial institutions to develop a written formal plan to protect the nonpublic personal data of its clients. Of particular note are new regulations within the Health Insurance Portability and Accountability Act (HIPAA) that cover the use and disclosure of patient health information. A provision of the recent American Recovery and Reinvestment Act of 2009 expands HIPAA compliance to business associates of healthcare providers, including attorneys and accounting firms. These associates are now responsible for HIPAA violation penalties which can reach as high as US\$1.5 million per calendar year and require notification of both the U.S. Health and Human Services department and a "prominent media outlet." Additionally, violators can face criminal charges with penalties that include imprisonment for up to 10 years.

Forty-four states have regulations requiring notification of affected parties when data breaches occur. Currently, Nevada and Massachusetts are leading the nation in encryption requirements for companies that store or transmit the personally identifiable information of its residents. Compliance extends to any business that manages state resident data, including businesses outside these states.

A sweeping new federal bill in process, the Personal Data Privacy and Security Act of 2009 (S.1490), if passed, may replace the patchwork of state regulations and would require companies and government agencies to follow specific rules for protecting sensitive and personally identifiable data.

## SECURE FILE TRANSFER (SFT) TECHNOLOGY

With the myriad laws and regulations, and with future legislation coming, companies must address significant changes to existing processes and workflows, and they must now make complex infrastructure and technology decisions to meet many of the data protection requirements.

For obvious reasons, law firms are searching for ways to send sensitive information with the assurance that it will not be intercepted and misused. E-mail, FTP and other existing tools and methods are not up to the task, and new solutions must be deployed by organizations to handle sensitive information. Companies looking for solutions to help them comply with current and future requirements should consider the following criteria when evaluating SFT products: ease of use, cost, reporting and support.

## SECURITY AND ARCHITECTURE

Always of paramount concern, strong security is necessary; ideally, it is unobtrusive to end users. Data breaches may not only entail monetary fines, but in many cases can hurt a firm's reputation when word gets out that confidential data is not being handled properly and securely.

- **Is data encrypted when transmitted over public networks (in transit) as well as when it is being stored (at rest)?**
- **Are recipients of a secure file transfer properly authenticated?**
- **Can files sent to the wrong recipient be recalled?**

Hand in hand with security, the overall system architecture can play a positive or negative role in security. An all-in-one solution that may have to sit close to, or even within, a public-facing network tier is more vulnerable to attack. A framework that supports splitting an application into tiers where the user interface is publicly facing, but the data is located in a more protected network segment, has significant advantages. Flexibility in deploying a solution is important for IT architects who might have specific security requirements for new applications.

- **What kind of system architecture does the solution support? Can the application be separated into logical and physical tiers?**
- **Are there any special client requirements, or does the solution support thin clients like Web browsers?**
- **Will the application run on multiple platforms?**
- **Is the application compatible with virtual environments; or, better yet, is the solution available as a virtual appliance?**
- **Can administrators tie into their existing directory services (AD, LDAP) for user management and authentication?**

## USABILITY

Perhaps the most critical aspect of an SFT solution is usability, primarily because overly complex and confusing tools are often not used, thus defeating the solutions' purpose. Even worse, those users who refuse to apply the available security measures to share data may revert to traditional file transfer mechanisms, or even post information to an external, unsecure file-sharing site. When determining ease of use, it is important to keep in mind that minimizing changes to user behavior can help increase adoption of a new application.

- **When sending files, does IT need to get involved, or is the solution self-service?**
- **How difficult is the system to use for people on the receiving end of secure file transfers?**
- **What kind of training is required to get an end user up and running? Can someone start using the system with minimal instruction?**
- **How flexible is the system, and can it be tailored to the firm's particular environment and requirements?**

## **COST**

With tighter corporate budgets the norm these days, buyers are looking for more value from their solutions. Often vendors hide costs by selling a base system that requires additional modules or features that are offered *a la carte*. This can drive the purchase price well beyond initial quotes. Buyers should pay close attention to add-on costs, hidden fees, *a la carte* pricing, as well as licensing terms. Are user licenses annual or perpetual? A useful exercise is to compare products over a three- to five-year period to capture recurring costs when calculating total cost of ownership.

In addition, since most companies already have investments in storage, computing resources and databases, leveraging these resources can keep overall costs low and increase utilization of existing assets. For example, it is a good idea to see if the infrastructure can be used in conjunction with the SFT system to utilize the firm's storage area network (SAN) or network-attached storage (NAS) for file storage.

## **REPORTING**

Many federal, state and industry regulations require regular audits. Detailed logging, coupled with a robust reporting system, can facilitate third-party audits. Being able to verify the successful receipt of a message or file gives senders important feedback that they've closed the loop. Evaluating the reporting feature of a secure file transfer solution should include ensuring the level of logging detail is granular enough for the firm's needs.

## **SUPPORT AND SERVICE**

Unfortunately support, or lack of it, is often only discovered post-purchase. But established companies with a long history of recognizable customers can be an indicator of a trusted vendor. Buyers should see how

willing the vendor is to listen not only to support issues, but also to feature requests.

## **CONCLUSION**

Navigating the data privacy waters can be daunting, but understanding an organization's needs and applying the criteria listed above can help ensure that a secure file transfer solution is well suited to the organization's file transfer needs and also meets regulatory requirements. **ILTA**



Bill Ho is the Vice President of Internet Products for Biscom where he is responsible for product management of Biscom Delivery Server, a secure file transfer solution. Previously, Bill was CEO and founder of vVault. Bill received a BS from Stanford University and an MS from Harvard University, both in the field of computer science. Bill can be reached at [bho@biscom.com](mailto:bho@biscom.com).