

SECURE AND MANAGED FILE TRANSFER IN THE ERA OF REGULATORY COMPLIANCE

KEITH PASLEY, CISSP

Information security professional specializing in helping companies understand security requirements related to regulatory compliance and how these requirements affect their product strategy.

SPONSORED BY IPSWITCH FILE TRANSFER

ABSTRACT

Today's economy is increasingly based on information flow. Getting the right information to the right person at the right time is the key strategy for business success. It is critical that the execution of this strategy ensures that the storage and transfer of information is reliable and secure.

File transfer as a business process must provide end-to-end visibility, security, auditability and compliance management. Increasing regulatory compliance and government mandates such as HIPAA, PCI DSS, Sarbanes-Oxley, Gramm-Leach-Bliley, BASEL II, J-SOX and FIPS are compelling companies to establish a management strategy that includes the file transfer process, integrates into existing compliance processes and minimizes cost of compliance to the bottom line.

A secure and managed file transfer approach can help companies better meet the challenge of safely and reliably exchanging electronic business information.

“Advantage can be gained by utilizing software that comes with a variety of built-in secure application controls that improve consistency of operation, automate reconciliations, facilitate exception reporting, and support proper segregation of duties. Commercially available packages also bring advantage in the form of embedded facilities for controlling which employees can access or modify specified data, performing checks of processing completeness and accuracy, and maintaining related documentation.”¹

Unprecedented changes have occurred in recent years that affect the fundamental way companies conduct business. Insidious threats to the security and reliability of critical data and business processes and the increasing velocity of privacy laws and regulatory compliance mandates increase the risks of sharing information. Regulatory compliance and government mandates, such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and the Payment Card Industry Data Security Standard (PCI DSS), J-SOX (a variant of SOX), BASEL II and FIPS are forcing companies to document all their business processes. Information transfer is one major business process that is receiving increased scrutiny.

Indeed, a typical company may need to provide proof of compliance to a number of different regulators, business partners and customers. At no other time in history has the very existence of businesses depended so crucially on its ability to manage the secure transfer of business information while maintaining compliance.

Today’s economy is increasingly based on information flow. Getting the right information to the right person at the right time is the key strategy for businesses to be successful.

Summary of Common Compliance Mandates

Health Insurance Portability and Accountability Act (HIPAA)

Preserve the privacy and security of personal health records. HIPAA requires that companies prevent unauthorized access, alteration, deletion and transmission of electronically stored and transmitted health information.

Payment Card Industry Data Security Standard (PCI DSS)

Safeguard credit cardholder data and sensitive card authentication information. PCI DSS provides a minimum security standard for protecting cardholder data - both in-transit and in-storage - to ensure that members, merchants and service providers maintain a consistent and secure cardholder data environment.

Sarbanes-Oxley Act (SOX)

Protect public company financial information. Businesses must ensure the integrity of data used in public financial statements from malicious or accidental harm. The Securities and Exchange Commission oversees SOX compliance and it holds corporate officers responsible for financial statement accuracy.

BASEL II

Ensure the soundness and stability of the international banking system using risk management strategies. Information technology security is considered under the category of operational risk management in the BASEL II agreement.

J-SOX

Protect integrity of public company financial data. A Japanese draft legislation - soon to be law - similar to the objectives of the U.S.-based SOX that mandate use of a framework for internal controls over financial reporting systems (including the underlying information technology) by Japanese companies.

Gramm-Leach-Bliley Act (GLBA)

The Financial Modernization Act of 1999, also known as the “Gramm-Leach-Bliley Act” or GLB Act, includes provisions to protect consumers’ personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.

Federal Information Processing Standard (FIPS)

Federal Information Processing Standards (FIPS) are publically announced standards developed by the United States Government for use by all non-military government agencies and by government contractors.

Standards for The Protection of Personal Information of Residents of the Commonwealth (201 CMR 17.00)

The standards to be met by companies who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records.

¹ Internal Control over Financial Reporting-Guidance for Smaller Public Companies”, Committee of Sponsoring Organizations of the Treadway Commission, June 2006. Available online: <http://www.coso.org/publications.htm>; last accessed 5 February 2007

When applying this strategy, file transfer, the technology-based process of uploading or downloading information both internally and externally, becomes a mission-critical component of an information-rich business process.

Successful execution of this strategy means businesses must be able to manage the information flow and maintain end-to-end control over all aspects of information movement between any two entities. It is critical that the execution of this strategy ensures that the storage and transfer of information is secure and reliable. The confluence of internal and external threats translates into increased operational risk to the successful execution of your business strategy. These merging risks include:

1. The security and reliability of the information exchange process
2. Pressure to increase efficiency while reducing business IT costs
3. Maintaining regulatory compliance

The increasing number of regulatory compliance mandates has introduced a level of security and risk into business management, processes and information-security practices as never before experienced. If you are not prepared to manage these compliance risks you will not be able to take advantage of new business opportunities — and in some cases, it will cost you from continuing with your existing business. Companies that clearly understand these profound changes and how to use new approaches stand to gain the most competitive advantage.

The good news is that companies can take steps to reduce the inherent business risk of sharing data by using file transfer solutions and best practices that are not only reliable and secure but also increase efficiency by integrating with existing business workflow processes.

A new class of secure and managed file transfer solutions help in meeting the challenge of managing and securing the transfer of information between two or more entities. To truly understand the significant changes underway and how secure and managed file transfer solutions can help we have to look back to where file transfer began.

EVOLUTION OF INFORMATION SHARING – SIMPLE TO COMPLEX

Electronic information exchanges using the standard File Transfer Protocol (FTP) as a business communications tool is not new. What has become the standard FTP protocol commonly used today began as a group of protocol specifications which described a method for generalized, reliable file transfer between computer systems. FTP uses two communications channels, or ports, for sending and receiving data. Developed in the early 1970s at MIT, the FTP protocol eventually was formalized as a standard protocol by the Internet Engineering Task Force (IETF) as described in the Request for Comment (RFC) 959² in 1985. Today, FTP continues to be heavily used as the backbone of information exchange by most businesses around the globe.

Since the original specification included minimal, if any security, as its use increased and the Internet became more and more open, problems were encountered with the protocol. For example, the standard FTP specification did not include the use of strong authentication, such as encrypted passwords or

² “RFC 959 -File Transfer Protocol”, Information Sciences Institute, October 1985. Available online: <http://www.wu-ftpd.org/rfc/rfc959.html>

authentication tokens. Sending the login credentials in clear text allowed cyber-thieves to sniff login information which could then be used to gain unauthorized access to data. Even worse, the standard FTP did not provide for encrypting the files being transferred. Unencrypted file transfer, which could potentially allow a man-in-the-middle attack³ and unauthorized viewing of data either during transmission or in storage on the server, has become a huge privacy concern today. Today, FTP enables file movement between disparate devices and systems but, by itself, does not provide strong security, data management, monitoring, or process control needed for businesses with critical security requirements.

Along with the rise in use of FTP, and as companies became more comfortable with information technology, file transfer via electronic mail (email) became a common business practice in the mid-to-late 1990s. A shared goal of FTP and email is to use technology to compress time and distance by electronically sharing files. However, transferring files as attachment to an email message is not scalable, inefficiently consumes email server resources, and yields poor data management over file attachments themselves.

Similarly, a relative newcomer to the information sharing market is instant messaging (IM). IM is a form of electronic communication that enables two or more individual network users who are simultaneously online to exchange messages in real time. Businesses have seen the benefit of IM use as it further reduces time and distance similar to traditional telephone use for quick communications without the intrusiveness of a telephone call. Some IM programs allow for file transfer. However, as in the case of standard FTP and email, security is a big issue with IM. Managing information flow to ensure that that IM users are being securely identified and authenticated, that inappropriate messages and data files are not being exchanged, and that all communications are being properly encrypted are a just a few of the security and data management risks that companies face when considering IM as a file transfer option.

Given the information-sharing challenges facing IT executives today, neither standard FTP, nor standard email, nor the current crop of IM products are ideal options for managing secure file transfer.

PRIVACY BREACHES – THE CASE FOR ENCRYPTION

It is estimated that over 200 million records containing sensitive personal information have been exposed to unauthorized disclosure due to weak or non-existent security since January 2005⁴. Many

Email: Not Encrypted, Not Private

The convenience of email as a means for transferring files has contributed to its enormous popularity as a business tool. However, when security and efficiency are imperative, email may not be the best choice. Unless files are explicitly encrypted, email attachments are susceptible to being intercepted and viewed by malicious users while in transit. Additionally, email systems use “store and forward” technology, a technique in data communications in which data are stored at some point(s) between the sender and the receiver and are later forwarded to the receiver.

Typically, email messages are forwarded through servers/devices across the internet with residuals of the message left behind at the intermediate servers/devices out of your direct control. Any information in the files - from sales figures, to patient records, product designs, and legal records - is vulnerable.

Also, standard email does not require strong authentication of the user or the data, therefore anyone can send an email to any email address without verification of the integrity of the message or the sender. However, not everyone can transfer a file to a secure ftp server unless they are specifically allowed.

In addition to the security risks, email is also not well suited for transferring large files. If a company relies too heavily on sending large files via email, the mail server performance and the network is resides on will deteriorate, affecting the timely delivery of all email large and small. To combat this, some administrators implement rules that disallow email attachments over a certain size, such as 10MB, or type, such as Zip files. These policies further limit the practicality of email for file transfer. Not only will large files not be delivered, but in many cases they will be returned to the sender, placing additional burden on the sender's email system. Also, email attachments have the potential to be mistakenly blocked as spam. In such cases, the recipient may not even know that the file was sent, and the sender may not know that the file was not received or received with compromise. Email when used as a file transfer vehicle is inefficient and insecure.

³ “Man-in-the-middle-attack”, Tippet Inc IT Security, 2006. Available online: “<http://www.itsecurity.com/security.htm?s=515>”

⁴“A Chronology of Data Breaches”, Privacy Rights Clearinghouse, April 2005. Available online: <http://www.privacyrights.org/ar/ChronDataBreaches.htm#Total>

of the reported breaches could have been prevented by the use of encryption and/or content security controls.

Two regulations that are driving the increased use of encryption are state privacy/disclosure such as California Senate Bill 1386 and the Payment Card Industry Data Security Standard (PCI DSS). If an organization detects an unauthorized exposure of a specific combination of private information on California residents it must notify the individuals unless the exposed data is encrypted. Within the retail and credit card industries, the PCI DSS regulation strongly recommends merchants encrypt all card holder information and transactions across open networks.

A robust secure and managed file transfer solution must provide strong encryption using well understood algorithms, cryptographic keys of appropriate length, and cryptographic modules that have undergone validation testing. Otherwise, the solution can not be trusted to assure the confidentiality of the data before, during and after the file transfer.

In addition, the state of your data can present an extra security challenge. Data can exist in at least two different states. "Data-At-Rest" is the state data is in when in storage, on a server for example or when it's being stored locally on your laptop. "Data-In-Transit" is the state data when it is in motion, being transferred, for example, from your client laptop to a server or even from server to server. Both states, at-rest and in-transit, present opportunities for security breaches.

Data needs to be protected during both states. One way to protect data in either state is to apply cryptography to the data in either state. Two well understood encrypted transfer protocols for protecting data during the file transfer are Secure Sockets Layer (SSL) protocol and Secure Shell (SSH) protocol.

Complimentary encryption layers deliver bullet-proof secure file transfer.



Additionally, OpenPGP provides an additional level of protection for data-at-rest or data in storage and Secure Hash Algorithm (SHA) helps to guarantee delivery and validate that transferred files have not been compromised. Many security experts recommend combining (1) SSL or SSH protocol transfer encryption with (2) PGP file encryption to ensure that files are protected before, during and after transfer. The combination of these provides overlap to ensure minimal risk of unauthorized disclosure of your sensitive data during all phases of file transfer process. These encryption methods enable the secure transfer and storage of files and data.

SECURE SOCKETS LAYER (SSL) - TRANSPORT ENCRYPTION

SSL, also known as FTPS or “Secure FTP over SSL” can be used in conjunction with FTP to provide secure encryption over standard FTP connections. The SSL protocol enables encrypting and decrypting of FTP sessions across networks to provide authentication of credentials and secure private communications. When an FTP client makes an SSL connection with an FTP server, all data sent to and from that server are encrypted using various strengths of complex mathematical algorithms. Encryption algorithms make it difficult for attackers to read intercepted data. The recipient must have the corresponding decryption key in order to read the file.

SECURE SHELL (SSH) - TRANSPORT ENCRYPTION

SSH, also known as SFTP or “SSH File Transfer Protocol” is a popular protocol that delivers secure communications and is used for secure and managed file transfer. It uses Secure Shell 2 (SSH2), a secure tunneling protocol, to emulate an FTP connection and provide a secure and encrypted channel for file transfers. It is particularly popular in IT environments because most operating systems (including UNIX/Linux) support SSH and using SFTP allows for IT standardization. SFTP is very firewall friendly because it uses a single port for uploading and downloading, and it improves on the security of standard FTP by encrypting all data transfer traffic, connection data and passwords to eliminate eavesdropping, connection hijacking, and other attacks. As an added bonus, it also compresses all data during the transmission which can result in optimized file transfers. Another widely used feature of SSH is Secure Copy (SCP2). It provides interoperability across multiple operating systems and platforms and includes desktops, servers and mainframes.

PRETTY GOOD PRIVACY (PGP) - FILE ENCRYPTION

Despite its somewhat underwhelming “Pretty Good” name, OpenPGP delivers very strong and secure encryption at the file level. OpenPGP, a type of Public Key Infrastructure (PKI), is also known as IETF RFC 2440. While SSL and SSH encrypt data while in transit, OpenPGP is used to encrypt individual files in storage. OpenPGP is an open standard that uses a system of public and corresponding private keys to authenticate users and data - sometimes called “key pairs.” An additional cryptographic key set, called the secret or symmetric key, is dynamically generated to encrypt the actual data file as it resides on a server. The intended receiver can only decrypt the file if they apply the same secret cryptographic key that was used to encrypt the file. OpenPGP file encryption is often used in conjunction with standard FTP, SSL or SSH transfers to ensure that files at rest are safely encrypted.

SECURE HASH ALGORITHM (SHA) - FILE INTEGRITY CHECKING

File Integrity Checking uses built-in file verification mechanisms to guarantee delivery and validate that transferred files have not been compromised in any way. Secure Hash Algorithms such as SHA-1, SHA-256 and SHA-512 are cryptographic hash functions designed by the National Security Agency (NSA) and collectively published as a US government standard. SHA technologies ensure that the source file and transferred file are exact matches.

WHERE DO WE GO FROM HERE? – THE CASE FOR SECURE AND MANAGED FILE TRANSFER.

Outmoded approaches to transferring files are no longer adequate. The modes of business information exchange have evolved from simple to complex.

Today, complexity is not only being driven by demand for information exchange solutions with integrated security and reliability. Businesses are now challenged with enabling communication flow of business critical data while maintaining regulatory compliance, and addressing privacy and risk management mandates.

Demand has increased for information exchange solutions that not only ensure the end-to-end security and reliability over the file transfer process but also provide management visibility over the file transfer process via integrated application level security, compliance reporting, auditing and work flow monitoring and automation.

Current solutions exist that implement the secure file transfer approach and allow businesses to:

- Reduce the cost and risk of providing access to critical data due to adherence to privacy and security regulations
- Simplify file transfer business process to better understand, monitor and quickly respond to changing business requirements
- Secure file transfer communications via embedded security
- Provide data management, monitoring and scheduling (including tracking auditing and guaranteed delivery)

SECURE AND MANAGED FILE TRANSFER – HELPING TO MEET THE COMPLIANCE CHALLENGE

SECURITY - THE UNIFYING FABRIC OF REGULATORY COMPLIANCE

Security is vital to compliance. Managing the end-to-end security and compliance of file transfer data and processes requires a proactive approach to security, reliability and compliance management. Security builds a safe, confident and auditable environment to support compliance. The security embedded in the file transfer server software that IT Administrators use to manage company data must be compatible with the file transfer client software that is being used to access and transfer files with the server. It makes the most sense for optimization to use the same client server from the same vendor to leverage optimization between the pair.

Secure and managed file transfer solutions help businesses proactively increase security assurance, maintain regulatory compliance and increase business productivity by applying embedded, multi-layered security and data management controls over the file transfer process.

COMPLIANCE STRATEGY - BEST PRACTICES FOR COMPLIANCE IN SECURE AND MANAGED FILE TRANSFER

Compliance increases cost for businesses. Compliance costs can be reduced or better managed by using a proactive compliance management approach.

Compliance management can be defined as the ability to⁵:

- Document a regulated business process
- Monitor the business process
- Measure and report on effectiveness of controls over the process

⁵ Mogull, Rich, Heiser, Jay "Information Security for Regulatory Compliance: What Matters Most?", Gartner IT Security Summit 2005, June 6-8 2005

If you have established a business process to handle regulated data and monitor the process for compliance, then assuming adequate reporting infrastructure, you can create reports showing the effectiveness of your security controls to auditors. Business scaling and cost efficiencies can be gained by leveraging monitoring and reporting systems across the enterprise. IT administrators, CTOs/CSOs, Chief Compliance Officers prefer secure and managed file transfer solutions that tie into existing reporting and monitoring using such management and monitoring protocols as Syslog.

What is needed is a strategy of supporting unified security requirements that commonly underlay most, if not all, regulatory compliance mandates. One cost effective approach to baselining the security requirements using this strategy is to identify the security requirements from all the various regulations that affect your company. Then categorize the common security requirements you have identified among the regulations that apply to your company. Finally, identify overlapping security requirements to form a baseline of compliance/security characteristics needed in your environment to support your compliance objectives.

As an example, an analysis of a sampling of the top regulations facing businesses today—Health Information Portability (HIPAA)⁶, Sarbanes Oxley (SOX)⁷, Financial Instruments and Exchange Law, J-SOX (a variant of SOX), International Convergence of Capital Measurement and Capital Standards - A Revised Framework (BASEL II)⁸, Payment Card Industry Data Security Standard (PCI DSS)⁹, and Gramm-Leach-Bliley Act (GLBA)¹⁰, Standards for The Protection of Personal Information of Residents of the Commonwealth (201 CMR 17.00)¹¹—reveal three common security characteristics: confidentiality, integrity, and availability.

TEN QUESTIONS TO TRULY UNDERSTAND THE RISKS OF YOUR FILE TRANSFER ENVIRONMENT

Do you know how well your current file transfer environment supports your business processes? Review the following ten questions to measure the effectiveness of your file transfer processes – and to better understand the risk you may be facing.

1. What business processes depend on the security and reliability of file transfer?
2. What is the file transfer workflow for each identified business process?
3. Does your file transfer technology architecture integrate well with your file transfer workflow?
4. Does your file transfer architecture provide secure, reliable, end to end visibility of your critical processes?
5. Who needs access to the information?
6. Where is the information stored?
7. Are there additional complicating factors such as regulatory compliance, privacy and SLAs?
8. Will you need to replicate file transfer services at a disaster recovery site?
9. Is file transfer included in your business continuity plan?
10. What would be the impact to your business operations due to a lack of availability of file transfers?

The answer to these questions will also depend on the type of operational environment the information resides in or traverses, whether or not the file transfer uses a distributed or centralized model, and the size of the business. As you answer the above questions consider any areas of weakness in file

⁶ "Security Standard", Centers for Medicare & Medicaid Services, February 2003. Available online: http://www.cms.hhs.gov/SecurityStandard/02_Regulations.asp

⁷ "Public Law 107-204", Securities Exchange Commission, July 2002. Available online: <http://www.sec.gov/about/laws/soa2002.pdf>

⁸ "Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework", Bank for International Settlements, June 2004 . Available online: <http://www.bis.org/publ/bcbs107.htm>

⁹ "PCI Security Standard" PCI Security Standards Council, September 2006 . Available online: <https://www.pcisecuritystandards.org/index.htm>

¹⁰ "Privacy Initiatives: The Greamm-Leach-Bliley Act" Federal Trade Comission. Available online: <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

¹¹ "Standards for The Protection of Personal Information of Residents of the Commonwealth" Massachusetts Government, January 30, 2009. Available online: http://www.mass.gov/?pageID=ocamodulechunk&L=1&L0=Home&sid=Eoca&b=terminalcontent&f=idtheft_201cmr17&csid=Eoca

transfer resiliency and then consider the secure and managed file transfer approach, such as Ipswitch file transfer products, as part of your remediation plan.

Without this level of understanding, your business is like a large ship at sea that sees only the tip of the file transfer “iceberg”. An example of what can go wrong when the file transfer process is not properly valued as strategic to critical business processes is Card Systems.

LACK OF SECURE FILE TRANSFER APPROACH DRIVES COMPANY OUT OF BUSINESS

Card Systems, a now defunct credit card data processing company, experienced every company’s worst nightmare in June of 2005. Hackers were able to steal thousands of credit card holders’ data from the company’s core FTP servers due to lack of strong network and systems security. As a result of what was found to be weak security and perfunctory adherence to a security standard, Card Systems was sanctioned with a multimillion dollar fine by the FTC. Even more deadly, their biggest customer representing over 90% of their revenue, Visa, ceased doing business with them. Card Systems, unable to recover from the compounded bad consequences of the security breach to their file transfer systems, was forced to go out of business in December of 2005. (See box on next page.)

Ipswitch Secure and Managed File Transfer Solutions Provide
<p>Confidentiality</p> <ul style="list-style-type: none"> • Protection of information from unauthorized exposure • Ensure the individual or process is who he/she claims to be before granting or allowing access through authentication • Provide need-to-know access to private information • Protect against unauthorized disclosure
<p>Integrity</p> <ul style="list-style-type: none"> • Assure accuracy and completeness of regulated information • Validate information during transmission and in storage on the server.
<p>Availability</p> <ul style="list-style-type: none"> • Ensure information is available • Safeguard file transfer resources such as load balancing and clustering
<p>Audit</p> <ul style="list-style-type: none"> • Document the effectiveness of security controls • Ensure separation of duties through configurable levels of detail • Enable Workflow automation • Provide visibility to file transfer process states with alert notifications

There are at least two lessons learned from the Card Systems story:

First, it doesn’t have to happen to your company. Second, it makes good business sense to include your file transfer work process when you perform an overall risk analysis of you business operations.

Do not underestimate or ignore the criticality of secure and managed file transfer to your core business processes. When executing the business strategy of information availability to the right person at the right time the stakes are too high and the risk to your business may be too great to do otherwise. Take an inventory of your file transfer needs, map it to the regulatory baseline security requirements and then find the right partner/solution to address them. Ipswitch File Transfer products embed the security capabilities of secure and managed file transfer and allow end to end visibility into all file transfer processes that support your critical business processes.

RECOMMENDATIONS

- Identify the business value of your file transfer infrastructure by performing risk assessment
- Include your file transfer servers in all risk assessments
- Use an asset-value based risk management strategy to determine how much to spend to protect information assets, including your file transfer processes, based on the assets' value to the successful execution of your business strategy
- Research and be fully informed of the regulatory issues related to your business or companies with whom you do business

IPSWITCH ENABLES SECURE AND MANAGED FILE TRANSFER

- Secure communications: Protect user information from unauthorized exposure with confidentiality measure that include Privacy, Access Control and Authentication
- Client/Server Solution: Ipswitch File Transfer clients integrate with and optimize the security functionality of Ipswitch Server Solutions
- Data management: Monitor and control data at-rest and in-transit, including logging, reporting and auditing
- File Integrity: Built-in file SHA-512 verification mechanisms validate that transferred files have not been compromised in any way and ensure that the source and destination files are exact matches
- Business process management: Create, manage and integrate into the file transfer workflow via automation, including scheduling, event notification, backup and high availability
- Standardize on your chosen file transfer client: Ensure that everyone who accesses your file transfer server is equipped with the same level of security and take advantage of economies of scales for user licensing, training and supportability costs

The Problem - Compliance does not equal security

In May 2005, computer forensics firm Ubizen traced an unusually large number of fraudulent transactions to credit card processor Card Systems. In June, Card Systems identified 239,000 credit card records that attackers had downloaded from its FTP server and warned that 40 million more may also have been compromised. In July, Visa and American Express announced that they would revoke Card Systems' right to process transactions on the grounds that the company stored customer data in violation of VISA and MasterCard's Payment Card Industry Data Security Standard (PCI DSS) rules. By September, Card Systems' remaining assets were set to be acquired by a rival.

So far, so simple. CardSystems was the bad guy, and the credit card companies acted quickly. But it wasn't quite that black and white. CardSystems later pointed out that it had actually passed a PCI DSS compliance audit, as required by Visa and MasterCard. It even tried to say the auditors were responsible for the mistake, claiming that they should have warned it of the security risks.

Blaming the auditors didn't wash with credit card organizations or the issuing banks. At the very worst, the auditors were complicit, just like Chicago based Author Andersen's role in the Enron saga. For their part, the auditors could say they hadn't seen any evidence of a PCI DSS violation. The Open Web Application Security Program top ten [Web Application Vulnerabilities] doesn't mention FTP servers at all, so Card Systems could even have been following the letter of the rules.

Behind all the buck passing, there are two serious lessons. First, compliance regulations isn't the same thing as business security requirementsSecond, reading a top 10 list isn't enough for application security.

SUMMARY

File transfer is part of the important information exchange business process. The increasing business risk due to regulatory compliance and the need for information everywhere business strategy emphasizes the need for secure and managed file transfer as the technological enabler for controlling the movement of data and the securing of data in-transit and as stored on servers. Further, to meet the global multi-regulatory environment that companies face today, security must be accepted as a business strategy and be embedded at the application level.

Proactive use of a unified compliance management strategy reduces the cost of compliance and increases competitiveness by not having to reinvent the wheel for each new regulation. Therefore, the

cost of compliance can be leveraged across multiple business processes to meet a variety of compliance objectives and process efficiency goals to quickly meet the changing regulatory landscape, faster than your competition.

Ipswitch file transfer solutions enable customers to proactively manage compliance of their file transfer business process by delivering a core set of industry leading security capabilities that meet and exceed the security requirements common to multiple regulations. A detailed analysis of how Ipswitch product features meet and, in many cases, exceed regulatory compliance security requirements is summarized here:

1. Confidentiality

- Authentication
 - Unique user IDs
 - Integrates with existing user databases
 - All passwords encrypted using strong encryption
- Access Control
 - Controls file access permissions
 - Implements separation of duties via role-based access control flexibility
 - Automate IP lockout with automatic blacklisting and whitelisting
- Privacy
 - Supports strong encryption such as 256-bit AES transfer encryption over SSL and SSH protocols,
 - Open PGP file transfer encryption and SHA-512 file integrity checking
 - FIPS 140-2 validated cryptography

2. Integrity

- Configuration files are encrypted
- Built-in file integrity checking
- Syslog to logging server support

3. Availability

- Supports clustering and load balancing
- Restarts interrupted file transfers where they left off
- Folder backups and file synchronization

4. Audit, Reporting & Logging

- Built-in Event Notification system
- Log Analyzer provides searchable view of logging data
- Syslog integrates into network and security management systems
- Optional: Software Developers Kit to integrate into custom applications

Every day Ipswitch solutions enable businesses to meet and exceed regulatory compliance and implement sound security policies by safely and reliably moving data across the Internet.

ABOUT THE AUTHOR

Keith Pasley, CISSP is an information security professional specializing in helping companies understanding security requirements related to regulatory compliance and how these requirements affect their product strategy. With over 20 years of experience in the information technology industry, with the last 11 years in information security, Keith has consulted with and designed security architectures and implemented security strategies for both government and commercial sectors. Keith is a security researcher and a contributing author to such publications as the Handbook of Information Security Management and the HIPAA Program Reference (both published by Auerbach). Keith has published articles on various security related subjects and provides consulting to firms looking to invest in the Internet security industry.

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 for more information on the Ipswitch File Transfer division and its range of solutions.

ABOUT IPSWITCH, INC.

Ipswitch develops and markets innovative IT software that is easy to learn and use. More than 100 million people worldwide use Ipswitch software to monitor their networks with Ipswitch WhatsUp®, transfer files over the Internet using the market leading WS_FTP® and MOVEit® brands of secure and managed file transfer clients and servers and communicate via Ipswitch IMail™ Server. Ipswitch values community involvement; visit <http://icare.ipswitch.com> to find out how to become involved. Visit www.ipswitch.com for more information on the company.



Contact Ipswitch's File Transfer Division