IBM Software
Smarter Commerce

Security best practices for file-based data movement—an IT practitioner's guide

By Rod Gifford, market segment manager – managed file transfer, IBM

IBM

Executive summary

Data security for file-based data movement is finally getting the attention it deserves. What was once a concern only in the financial services sector is now being treated seriously by all industries as they wake up to the liability and risk associated with the unsecured movement of files.

This rising concern, however, does not mean that companies have successfully mitigated the risk. According to a Privacy Rights Clearinghouse report, *The Top Half Dozen Most Significant Data Breaches in 2011*, "2011 was a significant year for data security, with some of the biggest data breaches in our history reported. So far in 2011, we've tracked 535 breaches involving 30.4 million sensitive records."[1] And there were probably other breaches that were never reported.

Although many companies have already recognized the need to protect data either in flight or at rest, much of their focus has been on applying narrow solutions to specific pain points. File-based data movement, however, is no longer as simple as moving files from point to point, system to system. The varied use of the Internet, cloud-based file transfer services, and individual or ad hoc file transfers as well as a reliance on the 40-year-old File Transfer Protocol (FTP) complicate the movement of files and make it more difficult for companies to protect the embedded data.

Supporting data security with the IBM Smarter Commerce approach

The IBM Smarter Commerce™ approach puts the customer back at the center of the business. And customers are more powerful than ever—equipped with mobile devices, connected through social networks, and capable of accessing and transmitting large data volumes in just seconds. Among these customers there is a growing demand for security and privacy as they share information. As more data is exchanged across a company's value chain, however, the risk to networks increases, and the potential for compromised data rises.

As companies seek to gain control and oversight over their file transfer activities, they need to consider adopting best practices based on the IBM Smarter Commerce approach. Although their immediate security concerns are likely focused on only internal and Internet-based file transfers, there is a larger opportunity for companies to establish best practices governing all file-based transfers, including those occurring across the Internet, through cloud-based services, and with internal or external point-to-point and person-initiated file transfers.

This white paper offers best practices to help companies protect their data using perimeter security, authentication, and the proper configuration and implementation of security policies. It also provides guidelines for the use of cloud-based file transfer services and person-initiated or ad hoc transfers. Ad hoc transfers, in particular, have become important because most companies have not implemented adequate controls and data protection capabilities.

Mitigating risk in a changing data security landscape

There are many reasons why protecting the file-based movement of data is critical to organizations. Ensuring timely implementation—and updates—of security policies that comply with government laws and industry regulations is one of the most compelling reasons to adopt security best practices for file-based data movement. But other factors can be just as important to organizations, including audit requirements, brand integrity, partner requirements and risk mitigation.

Indeed, the legal and financial risks can be immense. A Privacy Rights Clearinghouse report highlights a September 2011 data breach that exposed the Social Security numbers (SSNs) of 5.1 million TRICARE patients. The breach resulted in a US$4.9 billion lawsuit.[2] The case clearly shows the potential liability associated with data breaches and the impact on customers. In addition, the *2010 Annual Study: U.S. Cost of a Data Breach* study conducted by the Ponemon Institute found that the average per-incident cost of a data security breach in the United States was US$7.2 million.[3]

Unfortunately, many organizations lack a proactive stance in implementing data security measures. Instead, they react to each incident, drawing only from personal experience and gut instinct, not industry best practices. Respondents to the Ponemon Institute's *Best Practices in Data Protection* survey described their strategies toward best practices for data security in the following ways:[4]

- Nineteen percent have a formal strategy that is deployed across the enterprise.
- Twenty-six percent have a strategy that is partially implemented.
- Thirty percent have an informal strategy.
- Twenty-five percent have no data protection strategy.

An astounding 55 percent of the respondents lack a formal strategy governing the security of moving data. Is it surprising, then, to read that 2011 saw numerous, costly security breaches? In this age of the empowered customer, how many customers are willing to accept this level of risk?

To protect themselves, organizations need to safeguard their networks' trusted zones and their data, whether in flight or at rest. They need to protect data both within the enterprise and when exchanged with partners. And they need centralized security management to support security policies and best practices. Organizations must also consider regulatory and ownership issues. When transferring or storing files, it is essential to understand local and international regulations as well as who owns the data, where it resides, who has access to it and whether it needs to be encrypted.

As companies consider the adoption of best practices for file-based data movement, the emerging regulations and continuing occurrence of data breaches highlighted in the news should be enough to motivate a company to take action. What does not get enough consideration, however, is the importance of these best practices to an organization's value chain community. With a more customer-centric focus, companies would do well to use these best practices as a competitive differentiator for winning new business as well as a guide for protecting data that is shared across the value chain.

Getting started

Basic considerations

When considering governance and risk best practices, the first step is to identify the laws and regulations your organization must follow for the secure movement of data.

Which regulations apply to your organization and industry? Which apply to trading partner relationships? Examples include the following:

- Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Financial Institutions Examination Council (FFIEC)
- Health Insurance Portability and Accountability Act (HIPAA)
- European Union Data Protection Directive
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Odette for the automotive digital supply chain

After identifying applicable laws and regulations, create a scorecard to measure your effectiveness in complying with each requirement. Then identify gaps in coverage and prioritize initiatives to bring your organization into full compliance.

Consider the business drivers behind your file transfer activity as well as the underlying technology used both internally and throughout your value chain community. Understanding this landscape is important, particularly as more business transactions move to the Internet. A clear perspective on why and how data is transferred can help you recognize the variety of data and network security issues you face so you can apply appropriate best practices.

Organizational considerations also need to be taken into account. In many cases, the responsibility for data security rests with a senior IT manager or senior line-of-business (LOB) leader. In addition, many organizations establish cross-functional teams with IT and LOB representatives who can work together to recommend data security policies and monitor adherence to best practices.

Use case documentation

Start by identifying file transfer use cases that are critical to the success of your value chain and to compliance with each partner's data security requirements. The following table provides examples of typical file transfer use cases that may require some level of data security.

Industry	Use case example
Financial services	• Exchanging Automated Clearing House (ACH) transactions between banks • Exchanging credit card transactions between financial institutions
Retail	• Uploading daily sales information from stores to headquarters • Clearing credit card transactions between financial institutions
Manufacturing	• Distributing production plan updates to plants, suppliers and comanufacturers • Sending payroll data to third-party processors
Distribution	• Exchanging orders, shipments, receipts and inventory statuses with customers, suppliers and third-party logistics partners
Insurance	• Exchanging policyholder information with state agencies and healthcare providers
Communications and media	• Capturing order information from partner channels

Table 1: Examples of file transfers by industry

When documenting use cases for file-based data movement, the following questions should be asked:

- What data is moving? Where and how is it being moved?
- What is the sensitivity or risk level associated with the data?
- What is the business process disruption impact (may or may not have service level agreements [SLAs] tied to it) if the data is not delivered on time?
- What's the financial impact if the data does not get delivered?

A foundation of industry best practices

In this section, you will find lists of specific best practices for data protection, perimeter security, authentication, configuration and implementation of security policies, use of cloud-based file transfer services, and person-initiated or ad hoc transfers.

Data protection

- Understand the privacy policies of countries in which you operate or through which your data moves.
- Establish policies to control what types of data can be moved outside the country in which you operate and by whom.
- Establish the means to document where the data physically resides after it leaves the boundaries of the countries in which you operate.
- Realize that no data should be written or stored in the demilitarized zone (DMZ).
- Institute controls to help ensure data integrity.
- Adopt strong encryption options, including adherence to Federal Information Processing Standard (FIPS) regulations.
- Support Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.
- Interface with hardware security modules (HSMs) to store cryptographic keys for added protection.

Perimeter security

- Use a DMZ-based proxy.
- Prevent direct connections between the Internet and safeguard internal servers by terminating incoming communication sessions in the DMZ with SSL session breaks.
- Establish sessions from the DMZ to the trusted zone only after a partner user is properly authenticated.
- Do not store any data, files or user credentials in the DMZ.
- Do not require inbound hold in the firewall.
- Do not leave web services or user interface (UI) ports open in the DMZ.
- Try to make sure that data traverses from more-trusted to less-trusted zones.
- Conduct multiplex sessions through a single tunnel.
- Use protocol inspection, command filtering and blocking of common URL exploits to protect against malicious attacks.

Authentication

- Authenticate users in the DMZ rather than in the trusted zone.
- Manage users centrally in an external user repository such as a Microsoft Active Directory database.
- Use multifactor authentication, verifying users with "something you know" and "something you have" requirements.
- Use a logon portal for single sign-on.
- Adopt a logon portal that provides a self-service tool for user password management to decrease help desk support costs.
- Provide role-based access.

Configuration and implementation

- Deploy an architecture that minimizes the DMZ footprint.
- Address the needs of both security and network infrastructure teams.
- Provide operational continuity and high availability with options for clustering and load balancers.
- Support the ability to modify the configuration as security and network requirements change without purchasing additional components.
- Offer scalability to support growing file transfer needs.
- Use SSL to safeguard connections between solution components and any internal servers in the trusted zone.
- Leverage deployment options for a multitier DMZ.
- Use logging to track session activity and events in real time for audit, compliance and troubleshooting purposes.

Cloud-based file transfer service providers

- Define SLAs to help monitor the performance of file transfer activity flowing through third-party services.
- Ensure that third-party providers maintain their own security controls.
- Support data privacy by understanding who has access to vendor data centers.

- Revoke immediately the access credentials of employees who leave the company.
- Be willing to let your auditors conduct onsite audits.
- Make sure that data rests only in countries approved by your policy.
- Outline the use cases and data types that are acceptable for international transmission.
- Require an architecture that prevents other clients from gaining access to company data.
- Make sure that the architecture is up-to-date with security patches at all times.
- Provide a clear approach to removing and returning data when you leave the service.

Person-initiated or ad hoc transfers

- Establish clear policies on the types and sensitivity levels of data that can be attached to emails or copied to thumb drives.
- Deploy data loss prevention technology to trap sensitive data before it leaves the organization. For example, scan for SSNs or credit card numbers in email attachments or FTP files.

File transfer patterns and security risks

The following table catalogs typical file transfer patterns and potential risks to the data transferred. Note that the point-to-point pattern listed below is not new. However, the use of cloud-based services for file transfers is a recent development, and it introduces an additional set of risks that every organization must consider.

File transfer pattern	Description and technology used	Data security risks
Point to point (application to application)	• The application initiates the transfer. • A server-based application sends or receives files.	• Commonly uses FTP, which carries inherent security risks • Lacks encryption, so anyone with access to the files can view the content
Point to point (cloud based)	• The application initiates the transfer. • A cloud service provider facilitates the data transfer.	• Gives no control over the provider's technology • Relies on the provider to offer data security • Provides no control over where the data is physically located and who has access to it
Business to business	• Files are exchanged with trading partners over the Internet. • The process relies on mailboxes or a server-based file directory to send and receive files.	• Exposes the data and internal networks to security risks • Commonly uses FTP, which carries inherent security risks • Lacks encryption, so anyone with access to the files can view the content • Supports only basic authentication (login, password), which occurs inside the firewall • Involves sessions that are directly connected to your perimeter server
Person initiated (ad hoc)	• An individual initiates a file transfer to a person, email address or server-based file directory. • The process includes email attachments, FTP scripts and thumb drives.	• Bypasses network security controls, allowing sensitive data to move internally and externally • Lacks encryption, so anyone with access to the files can view the content

Table 2: File transfer patterns and their security risks

Implementing best practices

After you have established best practices, you need a plan to roll them out. Start with the compliance gaps you identified earlier and prioritize them according to criticality and level of effort required.

Select projects initially that are not only easy to implement but also likely to help kick-start organizationwide awareness and enforcement of critical security policies, such as those governing passwords or internal information sharing. These first projects should not require large time commitments or capital expenses.

Identify other projects based on gaps and priorities, and highlight technology solutions and recommendations when appropriate. For example, as employees use the Internet more frequently for information exchanges with partners, the need for a DMZ-based security solution will likely intensify, placing the project near the top of your project list. In all cases, you should develop budget estimates and work with IT and LOB sponsors to obtain the funding and approvals to start.

Technology requirements

Technology is a key piece of any security project, and you will need a plan to deploy it. First, identify the technology required to support the plan and create a budget for procurement and implementation. Many point solutions are available, depending on your use cases and data security requirements.

When evaluating security solutions, assess your requirements for scalability, performance and support. Global operations will require a vendor that has strong global capabilities and ample capacity for large data volumes and high support expectations. Consider also that your security capabilities must be integrated into your file movement strategy, and determine whether you need a point solution to solve a particular issue or a broader set of capabilities across your file transfer infrastructure. This perspective will help you decide whether to engage with a single vendor or to use multiple vendors.

Many forward-thinking organizations are choosing to adopt a broader set of capabilities and leaning toward a single-vendor approach, avoiding the potentially high total cost of ownership associated with a multivendor strategy. Indeed, 40 percent of the respondents to the Ponemon Institute best practices survey indicated a preference for a single-vendor sourcing approach.[5]

Education and awareness

For effective adoption and enforcement of file transfer security policies, it is critical to provide education and drive awareness throughout the organization. Employees should understand why security is important—that it protects the company's brand and serves the best interests of valued customers. A security breach, especially when handled improperly, can permanently damage customer relationships and tarnish the company's reputation. Plans should be made to educate employees about the ways in which data can be exposed unintentionally and what they can do to minimize risk and protect the brand and value chain relationships.

Remember that *how* you educate employees can be as important as what you teach them. Pay close attention to your communications strategy and message, tailoring the material to make it relevant to employees' daily responsibilities. Make sure to incorporate testing into your educational plans to validate each employee's understanding of your data security policies.

Many organizations meet monthly or quarterly until best practices are implemented fully and then meet annually or in response to changing conditions such as new or updated regulations. Some forward-thinking organizations have established managed file transfer centers of excellence. A center of excellence makes it possible to take a more strategic and architectural approach to rationalizing, deploying and managing file transfer technologies, incorporating them into a broader IT security strategy.

Security audits

Not every best practice presented in this white paper will apply to your organization. That is why it is important to assess your security needs with the help of an auditor. Review sessions with auditors can help clarify which internal policies to implement, how passwords should be managed, whether cloud-based services should be audited and how often, and what metrics should be tracked. These metrics should incorporate file transfer performance and measure adherence with SLAs. To help ensure accountability, it may be necessary to associate a management-level review with certain metrics. Using these metrics, you can identify, prioritize and monitor projects that are focused on security gaps or risk mediation to help ensure success.

Convincing the business

One of the most critical parts of implementing best practices for security of file-based data movement is making the business case. To make an effective case, start with an overview of the overwhelming need for this type of security, and then hone in on which specific practices apply to your organization. Explain how the practices relate to the organization's overall data security plan and expand their relevance, including how they help satisfy audit requirements. Be sure to cover the value and benefits to the organization, including the potential impact of a security breach on the organization's brand and pocketbook and the importance of the issue to your value chain community.

Highlight any past damages, if applicable, or talk about other organizations in your industry that have suffered adverse events. Mention that data security best practices can be used as a competitive advantage with trading partners, can facilitate compliance with laws and industry regulations, and can help protect sensitive data as it moves internally or externally.

Share insight on what is driving other organizations to adopt their best practices. According to the best practices survey by Ponemon Institute, companies that take a best practices approach to data security do so for three primary reasons:[6]

- Twenty-six percent—to achieve substantial compliance with internal policies, procedures and agreements
- Twenty-five percent—to achieve substantial compliance with regulations, laws and public standards
- Twenty-one percent—to be an industry leader for data protection best practices

So compliance and a desire for industry leadership appear to be drivers behind the adoption of a best practices approach to data security. Recent trends confirm that pattern as various government agencies continue to push new mandates. The Information Commissioner's Office in the United Kingdom released a document, *Guidance on data security breach management*, to help companies prepare for handling security breaches.[7] And the U.S. Senate Judiciary Committee recently cleared three security bills that would require a "federal standard for notifying individuals of breaches of sensitive personally identifiable information."[8]

The most effective way to sell data security best practices to your organization is to obtain executive sponsorship. When the 2011 Ponemon Institute best practices survey looked at what distinguishes a company using data security best practices from other mainstream organizations, executive sponsorship stood out as a key factor. According to the study, "Organizations with best practices are better able to secure C-level and senior management support and funding because there is a greater responsibility for the protection of information assets and a desire to protect the company's good reputation."[9] The lesson? Best practices organizations that take a proactive view of data protection and don't wait for external factors to push them into action may be better positioned to respond to a breach, to support new compliance mandates and to be seen as industry leaders.

The goal is to avoid becoming yet another example of a data breach and suffering the potential multimillion-dollar cost of remediating its impact. Companies that deploy best practices around the security of file-based data movement seem to have an edge in that respect.

Why IBM?

Once you have a guide in place for the best practices you want to implement, you need to align those best practices with the appropriate technology solutions, which for file-based data movement are classified as managed file transfer solutions. As you consider your technology requirements, do not overlook the opportunity to lower your total cost of ownership by consolidating on a single vendor's products.

At IBM, we believe that security should be intrinsic to your business processes, development and daily operations. It should be factored into the initial design of your IT platform and critical infrastructure solutions, not bolted on later. Whether they are implementing a DMZ-based proxy solution using IBM Sterling Secure Proxy or using IBM Sterling Connect:Direct® software, an industry-standard point-to-point file transfer protocol whose security has never been breached in more than 25 years of use, companies can use IBM technology to help ensure the security of their data and networks.

At the same time, the age of the empowered customer places more emphasis on data security and requires trading partners to embrace a more security-conscious approach to protect data and internal networks. Taking a customer-centric approach to the development of file-based security best practices can help organizations ensure that policies align with value chain processes.

As part of the IBM Smarter Commerce approach, value chain synchronization requires strong business-to-business integration capabilities. One component of these capabilities is managed file transfer. A managed file transfer solution from IBM not only helps organizations achieve synchronization across their business communities; it can also provide a technical foundation for best practices.

For companies that want experienced advice on identifying and deploying managed file transfer technology, a Business Value Assessment from IBM offers a valuable option. As a collaborative engagement with IBM, the assessment can evaluate your current file transfer infrastructure and operational practices. It takes into consideration your organization's extended value chain and the entire file-based data movement required to keep it synchronized. IBM reviews the applicable best practices and helps align the technology, processes and IBM products that enable their use.

For more information

Contact your IBM sales representative to set up a Business Value Assessment or visit:
ibm.com/software/commerce/managed-file-transfer

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2012

1,2 Privacy Rights Clearinghouse, *The TopHalf Dozen Most Significant Data Breaches in 2011*, December 16, 2011, http://www.privacyrights.org/data-breach-year-review-2011

3 Ponemon Institute, *2010 Annual Study: U.S. Cost of a Data Breach*, March 2011.

4,5,6,9 Ponemon Institute, *Best Practices in Data Protection: Survey of U.S. IT & IT Security Practitioners*, October 2011, sponsored by McAfee, http://www.mcafee.com/us/resources/reports/rp-ponemon-data-protection-full.pdf

7 Information Commissioner's Office, *Guidance on data security breach management*, July 2011, http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Practical_application/GUIDANCE_ON_DATA_SECURITY_BREACH_MANAGEMENT.ashx

8 Harley Geiger, "Senate Judiciary Committee Passes Three Data Security Bills," Center for Democracy & Technology, September 23, 2011, https://www.cdt.org/blogs/harley-geiger/239senate-judiciary-committee-passes-three-data-security-bills

Please Recycle

ZZW03114-USEN-00