Progress® | ipswitch®

A PROGRESS WHITEPAPER

7 Steps to Compliance with Data Protection Laws

How Data Protection Regulations Apply to External File Transfers

Introduction

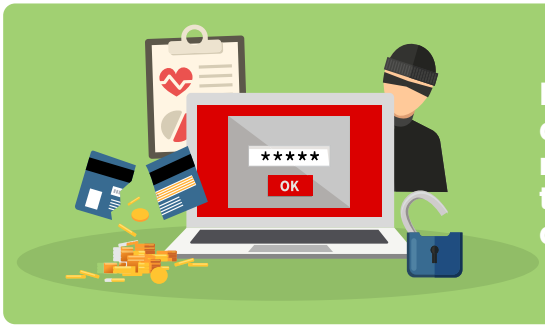
Stolen Personal Information (PI) drives a thriving black market for cybercriminals on a global basis. Since PI includes any data which can be used to identify an individual, every organization that collects data such as passwords, credit card data, health information and addresses is a potential target for cybercriminals. Not surprisingly, since 2013 data breaches have accounted for nearly 6 billion stolen data records globally. Also not surprisingly, governments around the world have responded with increasingly strict regulations regarding the collection, retention, processing and sharing of PI. Failure to comply with these regulations can result in severe fines.

The external transfer of PI is now a core operational business process across a wide variety of industries. IT organizations in industries such as retail, transportation, financial services, healthcare, entertainment, telecommunications and government as well as IT and business process outsourcers routinely collect, process and transmit PI. From a security perspective, data in transit is data at risk. IT teams must review their exposure to attack through the tools, technologies and processes they employ to externally share PI.

While data protection regulations around the world vary significantly, a small number of data security controls can go a long way to assuring compliance. This whitepaper will cover the seven security controls that are key to assuring regulatory compliance when transferring data externally

The Threat

Personal Information (PI) is typically defined as any data which by itself, or when combined with other data that the possessor can likely access, can be used to identify an individual. To a cybercriminal, access to PI makes organizations across a large number of industries lucrative targets for phishing, denial of service, ransomware and advanced persistent threat attacks.



Personal Information (PI) drives a thriving black market for cybercriminal tools, expertise and stolen data.

Since 2013 , global
data breaches
have accounted for
5.8 billion lost data records.

source: Breach Level Index

Since 2013, publicly recorded data breaches have accounted for over 5.8 billion lost data records globally. The data lost includes passwords, health records, billing addresses and credit information.

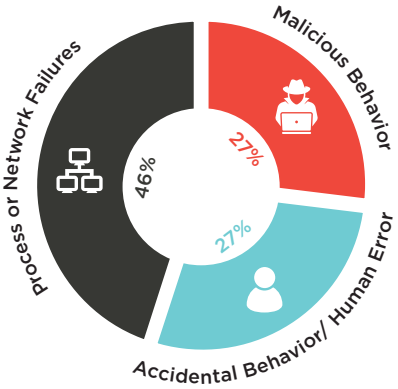
While no industry that collects and stores PI is safe, sources such as the Breach Level Index report that 80% of the breaches occur in the technology, retail, financial and healthcare sectors. If your organization collects, stores, shares, processes or transmits Personal Information, you are a likely target for attack.

Much of the stolen data makes its way to a black market where prices vary by data type and age (how long ago it was stolen). Per record prices for passwords may be .10 to .20 USD whereas recently stolen credit cards can be worth from 25 to 40 USD.

Geographically, very few nations are safe. While the US and EU combined accounted for 74% of the data lost since 2013, an additional 22 countries reported data losses in excess of 250,000 records in the same period. Leading the pack are China, South Korea, Turkey, Japan, Mexico, Canada and Russia with a combined total over 1 billion lost records.

The Enemy

Causes of Data Breaches



Who is responsible for these breaches? While the media would have us believe that the main culprits are nation states and cybercriminals, the truth is much less convenient. A recent Ipswitch survey of 255 IT professionals showed that only 27% of data breaches are the result of "Malicious Behavior". An equal percentage are due to "Accidental Behavior or Human Error". A staggering 46% of all data breaches were caused by "Process or Network Failures". We've met the enemy and they are us.

The truth is that most data is lost because someone within the organization or within a partner organization does something they should not. For example, data may be transmitted through unencrypted email attachments or via web-based file share services. Additionally, your or a business partner's employees may fall victim to a wide array of email or social media attacks.

In a recent email spoofing attack, employees of a healthcare organization were asked to respond with their EFSS user names and passwords – **60% complied.**

Sure there are those cases where large numbers of records are stolen through advanced persistent threats from cybercriminals, but even then, part of their attack chain usually involves an unsuspecting employee.

Your Risk Exposure

The first step in determining your organization's exposure to a potential data breach or non-compliance finding is to examine the systems and processes used to exchange data with external parties.

SCHEDULED FILE TRANSFER PROCESSES

Most likely your core file transfer processes, especially those involving PI, are already centralized to a small group of highly secured FTP servers. Hopefully, these use SFTP or FTPS which leverage SSH or SSL to assure encrypted transmission and authentication. Even SFTP/FTPS have limitations that expose you to an increased risk of security breaches and non-compliance.

Security/Compliance Risks of FTP

- **Lack of Encryption:** If the server is not SFTP or FTPS capable, file transmissions are in plain text (unencrypted) and vulnerable to theft in transit through a number of easy to use technologies.
- **Lack of Automation:** Repetitive manual file transfers leave organizations exposed to the risk of human error resulting in data loss. Scripts whose authors are no longer with the organization also pose a significant risk as they become outdated by process changes or updated security policies.
- **Lack of Visibility:** FTP servers often lack the degree of visibility and logging required by auditors. The logs should be tamper-evident and track file transfer dates, receipt by the intended party, and whether or not the file was subsequently deleted.
- **Lack of Scale:** Organizations often rely on IT to develop a collection of home grown scripts to automate their file transfer activities. As the needs of the organization grow, the scale and complexity of maintaining of these scripts become unwieldy and can introduce unanticipated security holes.

AD-HOC FILE TRANSFERS AND CLOUD-BASED TRANSMISSIONS

To maintain compliance with data protection regulations, your organization has to implement and monitor adherence to processes that assure the safe handling of PI. A particular vulnerability is the likelihood that an employee will transmit regulated data via an unsecured means such as an email attachment or via consumer-grade, cloud-based file share mechanisms.

IT organizations should pay particular attention to the use of unsecured file-share technologies by employees and external partners such as email, unencrypted FTP and consumer-grade cloud services.




Security/Compliance Risks of Email and Cloud-Based File Share

- **Encryption:** Files are not likely to be encrypted during transfer. This would be a clear violation of most data protection regulations.
- **Distribution:** There is no guarantee that transmitted data is only received by the intended recipient.
- **Data Life:** Files are not deleted and data may continue to be exposed months after the initial exchange. A healthcare provider was fined two million USD for leaving unencrypted data exposed to the public internet for two weeks.
- **Compliance in the Cloud:** Even when cloud-based file shares are advertised as 'compliant' the transmitting company is usually held responsible for assuring data security before, during and after the transmission.

File Transfer Security Controls

While the specifics of personal information protection regulations vary country to country, there are a core set of best-practice security controls that can help assure compliant file transfers. The ISO/IEC 27001 international standard, has been widely adopted across governments and industry sectors as it defines many of these best practices. The table below highlights the seven best-practice controls that are the most pertinent to external file transfer operations.

Security Requirement Control	ISO 27001 ref.	File Transfer
1. Compliance	A.18	Automation
2. Communications Security	A.13	Control & Visibility
3. Information Security Policies Security	A.5	Information
4. Access Control	A.9	Authentication
5. Cryptography	A.10	Cryptography
6. Physical & Environmental Security	A.11	Secure Architecture
7. Business Continuity Security	A.17	Failover

AUTOMATION

Commonly used file transfer workflows should be automated to mitigate against the introduction of human error that might result in data loss. Your file transfer tools should support functions such as automatic forwarding, error correction, and confirmation of receipt for all data transfers.

CONTROL AND VISIBILITY

Control and visibility of transfer activities are important security requirements and essential for validating compliance. Your tools should enable central visibility, control and prior authorization of all file transfers. Logs should be kept in a tamper-evident database to assure the integrity of audit trails.

INFORMATION SECURITY

Your technology, tools or processes should ensure file integrity checks, data deletion after receipt, and non-repudiation (the sender and receiver are both authorized and authenticated to access the data). They should provide an automated audit trail that tracks integrity, delivery and authentication

AUTHENTICATION

Effective authentication of users and administrators is an essential control. Your file transfer systems should accommodate an array of access control mechanisms, including integration with central user directories, role-based access control and single sign-on as well as multi-factor authentication.

CRYPTOGRAPHY

Encryption algorithms have a limited shelf life. Compliance standards often do not allow the use of compromised systems. It is essential that your systems employ strong, state-of-the-art cryptographic mechanisms and enable secure selection, distribution and protection of encryption keys.

SECURE ARCHITECTURE

Your systems architecture should integrate with existing security infrastructures and applications. The systems should also either ensure that there is no unencrypted data within the DMZ or provide for DMZ termination of inbound requests for authentication and data transfer with a gateway proxy server.

FAILOVER

A key requirement of many data protection regulations is secure business continuity. This requirement is meant to safeguard the confidentiality, integrity and availability of file transfers, at all stages throughout any failures, disasters or outages. Automatic, secure failover is essential to ensure that file transfers are either successful or continuously restarted until complete.

MOVEit Compliance Features

MOVEit® is a Managed File Transfer system that lets you manage, view, secure, and control the exchange of sensitive data with external parties to assure compliance with data protection regulations. The table below shows how MOVEit addresses each of the seven core best-practices for compliance with data protection regulations.

Case Study

How Medibank Secures Sensitive Information to Meet Health Industy Regulations

Security Requirement	MOVEit Control
Compliance	MOVEit helps ensure that file transfers are secured, data is protected at all times, and records of transfers are secured in tamper-proof audit trails for legally required periods prior to assured destruction.
Communications Security	MOVEit enables central visibility, control and prior authorization of all file transfers, as well as encryption, traceability and non-repudiation of transfers, including secure audit trails of significant events. MOVEit is architected to integrate with existing security infrastructure, policies, and applications, ensuring there is no unencrypted data in the DMZ and eliminating any requirement for external access.
Information Security Policies	MOVEit encrypts files at rest and in transit, provides non-repudiation and file integrity checks. Ipswitch provides email, web, mobile access and desktop clients which, when used with MOVEit provide compliant file transfer access to all users.
Access Control	MOVEit offers a choice of authentication mechanisms, including integrations with existing systems, and a rich set of features to support user access management, including blacklists and whitelists, and tools to help administrators select the most appropriate settings to meet security policies.
Cryptography	MOVEit employs strong cryptographic mechanisms and secure selection, distribution and protection of encryption and decryption keys, consistent with international legal and regulatory requirements.
Physical & Environmental Security	MOVEit provides flexibility in implementation to ensure adherence to local physical security requirements.
Business Continuity Security	MOVEit safeguards the confidentiality, integrity and availability of file transfers at all stages throughout any failures, disasters or outages. Ipswitch Failover can assure uninterrupted file transfer processing.

About Progress

Progress (NASDAQ: PRGS) offers the leading platform for developing and deploying strategic business applications. We enable customers and partners to deliver modern, high-impact digital experiences with a fraction of the effort, time and cost. Progress offers powerful tools for easily building adaptive user experiences across any type of device or touchpoint, the flexibility of a cloud-native app dev platform to deliver modern apps, leading data connectivity technology, web content management, business rules, secure file transfer, network monitoring, plus award-winning machine learning that enables cognitive capabilities to be a part of any application. Over 1,700 independent software vendors, 100,000 enterprise customers, and two million developers rely on Progress to power their applications.

Learn about Progress at www.progress.com or +1-800-477-6473.

Progress®
MOVEit®

Start your FREE TRIAL of MOVEit