Progress® | ipswitch®

A PROGRESS WHITEPAPER

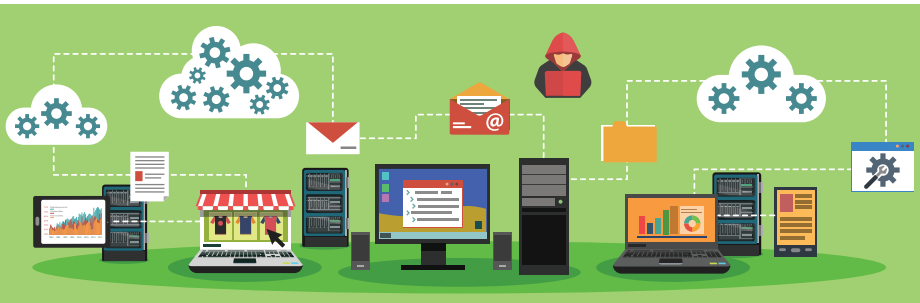
Banking and Financial Services Security and Compliance Considerations

Introduction

In an era when cybercriminals and nation states alike are continuously probing corporate security defenses, data protection safeguards become a necessity. Most of the data that banking and financial services concerns collect and store is highly valued on the black market. This makes your organization a top target for cyber attacks.

Therefore, your organization needs to implement policies and technology solutions that protect sensitive financial information as well as customers' and employees' Personally Identifiable Information (PII). Data such as social security numbers, bank account information, addresses, mortgage statements, and payment card numbers are considered sensitive and protected through a variety regulations. Failure to implement security operational controls sufficient to meet state, provincial and country regulations (or industry standards) can result in significant fines and loss of reputation.

Large portions of the data your organization operates with on a daily basis may also be transmitted outside the bounds of your secured network. Such is the nature of business today that data is routinely transmitted to outside vendors that provide key aspects of the financial services you offer to customers. While this information exchange allows your organization to deliver higher levels of service and capitalize on emerging growth opportunities, it also leaves you vulnerable to security breaches and data theft, loss or misuse.



Once sensitive data is outside the firewall, it is exposed to potential theft and misuse.

To protect their economies, governments around the world have implemented regulations controlling the security of financial information. With nearly 6 billion stolen data records globally in just the last 3 years, they have also implemented increasingly strict regulations regarding the collection, retention, processing and sharing of personal information.

Banks which operate in the U.S. must comply with multiple regulations containing data protection safeguards or provisions. The Gramm-Leach-Bliley Act (GLB) governs the collection and disclosure of customers' personal financial information and requires that financial institutions design, implement, and maintain safeguards to protect this information. For publicly traded organizations, Sarbanes Oxley auditing requires that 'internal controls and procedures' can be audited and that detailed audit logs are kept of all access and activity involving sensitive business information.

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

Globally, financial services firms that collect or store payment information with logos such as Visa, Mastercard, American Express or Discover must also comply with the Payment Card Industry Data Security Standard (PCI DSS). Over 32 countries, around the world, have some version of a Personal Information Protection Act (PIPA) which regulates the security of Personal Information (PI) or Personally Identifiable Information (PII).

In the US and other countries, banking and financial services organizations must also comply with state or provincial regulations. Any entity that collects, stores or transmits personal data concerning residents of the European Union must also comply with the General Data Protection Regulation (GDPR).

Many of these regulations contain important provisions requiring that sensitive data be protected not only by those institutions that collect it and store it, but also by external entities that receive or process that information. In other words, supplier and partner management is a critical component of your compliance strategy. Proper risk-assessment requires that you be aware of their security and compliance status as well as your own.

Most importantly, failure to comply with these regulations can result in severe fines.

Ensuring Data Governance

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

Organizations that rely on methods like Enterprise File Sync and Share (EFSS) and email to move data between partners, branches, and customers may find themselves in direct conflict with data protection regulations. While these methods are convenient, they usually fail to deliver the encryption, access controls and audit trails necessary for regulatory compliance. Organizations should also be aware that even when a cloud based service provider claims their product or service is 'compliant' with a data protection regulation, this does not mitigate your responsibility should the product be misused or the data ends up stolen.

Reliance on multiple FTP servers and platform dependent automation scripts to manage file transfers. As the number of systems used in file transfer increases, so does you exposure to the risk of attack. One of the key drivers behind IT teams consolidating to a single file transfer system is to reduce the number of potential attack vectors and simplify audit processes.

Compliance with regulatory mandates usually includes strong access controls, data encryption in transfer and at rest and log based audit trails. Internal security controls should also include requirements for standardized workflows that ensure data protection. To assure regulatory compliance, banks should replace ungoverned document transfer methods with secure, reliable, and compliant information exchange processes that ensure data security and integrity.

Two common security protocols that help secure and increase the reliability of data transfer are Secure Sockets Layer (SSL) and Secure Shell (SSH). Both are specifically designed to encrypt file transfers as well as the associated authentication data. SSL and SSH enhance the security and reliability of file transfer by using encryption to protect against unauthorized viewing and modification of high-risk data during transmission across open networks such as the Internet.

Data should also be protected both in transit and at rest (when sitting in storage to be opened or downloaded. Financial organizations should use the strongest commercially available cryptography for storing and transporting data. Combining SSL and SSH security with OpenPGP provides an additional level of protection for data at rest. OpenPGP encrypts files in storage through the use of cryptographic key pairs that authenticate users and data. Receivers need to use the corresponding private key in order to decrypt the file.

Secure Managed File Transfer

Secure Managed File Transfer systems enable external data transfers in a secure, accurate, controlled, and documented manner that addresses the full range of current and evolving legislative and regulatory mandates. They enable financial organizations to send data with return receipts and extensive tracking and auditing capabilities to ensure compliance GLB, PCI DSS, SOX, GDPR and other state, provincial or national regulations.

When evaluating Secure Managed File Transfer Systems or alternatives, you should look at how these offerings deliver against four categories—***confidentiality, integrity, availability, and auditing***—of features that contribute to compliance.

1

Confidentiality ensures that information can only be consumed by authorized individuals and only for approved uses. Confidentiality begins with authentication of login credentials and putting a strong password policy in place with features like expiring accounts and password management. Access control includes support for requiring 256-bit AES SSL encryption and TLS on all connections. This level of access should be mandatory for all clients connecting into your network infrastructure.

2

Integrity means ensuring you have uncompromised delivery of all correct data with full SHA support. Secure, encrypted data delivery is critical for ensuring business continuity. Secure hashing algorithms ensure that files have not been compromised during transport, and that the source and destination files are exact matches. Non-repudiation takes data security to the highest level currently available by adding digital certificate management to secure delivery and data encryption.

3

Availability can be achieved through load balancing and clustering architectures that support automatic failover and centralized configuration data storage to minimize the chance of a data breach. This also helps protect against distributed denial of service attacks. Availability can also be achieved by building checkpoint restart and robustness into the solution that can overcome hardware failures or interruptions in Internet connectivity.

4

Auditing provides comprehensive logging and log viewing with tamper evident security to guarantee the integrity of the log files. For technology, security, and other auditing purposes, all client/server interactions and administrative actions should be logged.

Progress® MOVEit® Compliance Features

MOVEit is a Secure 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.

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.

Download your FREE TRIAL of MOVEit