Meeting the challenge of compliance in financial services

Contents

The complex compliance landscape for finance

For much of the past two decades, and particularly since the global banking crisis of 2008, government regulators at home and abroad have made concerted efforts to regulate the activity of banks, lenders and other financial institutions. The compliance onslaught resulted in a veritable alphabet soup of regulations (GLBA, FFIEC, SOX, FSA, etc.) designed to ensure the resilience of critical financial institutions, reduce fraud and promote fair lending, all while protecting the integrity and privacy of consumer data.

These well-meaning regulatory requirements involve tremendous overlap and impose a significant burden on the financial institutions that must abide by them. Much of the cost and overhead of compliance in the financial services vertical lands squarely on information technology departments and, in particular, information security teams tasked with responsibilities like data classification, data protection, backup and recovery, and other core controls.

In this solution brief, we'll explore the roster of top compliance mandates facing financial institutions and their partners, discuss some of the requirements common to compliance in finance, and explore solutions from Trend Micro that help ease the burden of compliance for clients in the banking industry.

Key regulations and requirements for financial services

Along with healthcare, the financial services industry stands as one of the most heavily regulated verticals in the world. Dozens of global, national and regional mandates apply to banks, investment firms, loan companies and financial advisors.

While the exact roster of compliance requirements can differ by where a financial organization does business and the kinds of services it provides, there are a few regulations common enough to consider largely universal for any bank hosting transactions in the United States and the European Union. The ones with a strong information security component include:

GLBA (Gramm-Leach-Bliley Act)

Enacted in 1999, GLBA is a comprehensive law governing a wide variety of activities within financial firms ranging from employee policies to the organization and structure of investment and commercial banking units. Of interest to technology and security practitioners are the GLBA's provisions that

call for administrative, technical and physical controls to safeguard customer records and information.

Purposefully broad in scope, GLBA calls for organizations to do the following: "Develop, implement and maintain a comprehensive information security program that is written in one or more readily accessible parts containing administrative, technical and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."

FFIEC (Federal Financial Institutions Examination Council)

A formal U.S. government interagency body composed of five banking regulators, the FFIEC is, according to its charter, "empowered to prescribe uniform principles, standards and report forms to promote uniformity in the supervision of financial institutions." The FFIEC is made up of the Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC) and the Consumer Financial Protection Bureau (CFPB).

While the FFIEC has been around since 1979, the organization began working in earnest in 2014 to help make banks less vulnerable and more resilient to cyberattacks.

baseline and improve their alignment with security best practices.

SOX (Sarbanes-Oxley Act)

Enacted in 2002, SOX (sometimes referred to as Sarbox) aims to improve corporate and auditing accountability, responsibility and transparency for all U.S. public company boards, management and public accounting firms. While not strictly a financial services industry regulation, SOX is of special interest to financial institutions for two reasons: First, much of the ability to demonstrate compliance on the part of the regulated companies is dependent on the integrity of financial information held by the banks; and second, most of the large financial firms qualify for regulation as publicly traded companies themselves.

SOX-type regulations have since been adopted in Australia, Canada, France, Germany, India, Israel, Italy, Japan, South Africa and Turkey.

From the technologist's perspective, SOX is important mostly for its provisions regarding the ability to generate financial reports that are unambiguous and verifiable against source data. From an information security perspective, requirements under SOX revolve around maintaining data quality, detecting and responding to breaches, and attesting to the efficacy of security controls.

According to the FFIEC directives: "Information security policies, standards and procedures should define the institution's control environment through a governance structure, and provide descriptions of required, expected and prohibited activities … guide decisions and activities of users, developers, administrators and managers, and inform those individuals of their information security responsibilities."

In 2015, the FFIEC developed and released the Cybersecurity Assessment Tool, along with updates to its IT Examination Handbook to help financial firms measure their compliance

SOX also requires a control environment covering application development, change management, access to programs and data, and computer operations that are compatible with Committee of Sponsoring Organizations/ Control Objectives for Information and Related Technologies (COSO/COBIT) frameworks.

23 NYCRR 500

Among the newer regulations specific to financial services, the regulation known as 23 NYCRR 500 was introduced in 2017 by the New York State Department of Financial

Services (NYSDFS). The mandate applies to banks, lenders, trust companies and insurance firms doing business or licensed to operate in New York–which is to say all of them.

Similar to PCI DSS, 23 NYCRR 500 requires financial companies to implement a detailed, auditable framework to protect consumer data privacy and prevent data breaches. The rule calls for risk-based minimum standards for IT systems, including data protection and encryption, access controls and penetration testing.

Authentication and access management

Authentication standards vary, but the spirit of the financial regulations generally calls for an approach that aligns with the criticality and sensitivity of the data involved. Most established financial requirements dovetail with established guidance, such as the NIST cybersecurity framework (CSF), which calls for access to digital assets to be limited to authorized users, processes and devices, and to be managed consistently with the assessed risk of unauthorized access. As such, identities and credentials should be issued, managed, verified and revoked in accordance with established policy and audited for compliance.

Security and data protection responsibilities

Common among the major regulations governing financial firms are calls for the protection of sensitive information and assurances that data remains verifiable, immutable and well-defended against attack or theft. The fundamental concerns of the key governance mandates in the financial industry include:

Risk assessment and management

All of the main financial regulations include some provision for thorough, framework-based risk assessment that accounts for the financial firm's security controls environment, policies and procedures for security operations, threat models, vulnerability assessment and strategies for risk mitigation.

Data loss prevention

Maintaining the confidentiality and integrity of sensitive customer and transaction data is a top concern for financial regulators. Mandates call for robust data classification policies that earmark information based on its criticality and authorized uses. Once data is tagged, a combination of policies and technical controls must be maintained to examine file and data use across an organization's networks and hosts to protect against loss and unauthorized use or exfiltration.

Encryption

To information security professionals, encryption is regarded as another method of access control. To regulators, however, strong encryption is seen as a discrete data protection control. Regulations that require it call for minimum encryption standards, such as AES-256 or 2DES. They also mandate that encryption be applied to data at rest and in transit, which adds significantly to the complexity of the system for security teams.

Logging and auditing

Financial industry regulations come with a variety of rules regarding the retention of data and the requirement for producing information as necessary to support routine reporting and auditing. Most regulations call for a data retention period of three to five years, with some requirement for the destruction of old data once the reporting period has expired.

In most cases, retained data must include not only transaction information but also any other administrative data connected to the transaction, which, in the case of a transfer using a customer-facing web app, might include authentication events, source IP addresses, second authentication factors, risk-based decision values, decision logic results and query parameters, among other things.

Trend Micro solutions for financial services firms

Trend Micro delivers robust solutions that address the technical information security concerns discussed throughout this report and help organizations in the heavily regulated financial services industry reduce cost, combat fraud and ensure compliance. Trend Micro's Deep Security platform, for example, offers a comprehensive security platform that protects critical data and applications across all physical, virtual and cloud environments while addressing the majority of the financial industry's regulatory controls.

Available as an on-premises deployment or under a software-as-a-service model, Deep Security covers host-based security controls, intrusion detection and prevention, anti-malware, file integrity monitoring, vulnerability scanning, log inspection, end-user behavior monitoring, and other compliance-specific tools.

Tightly integrated with Trend Micro's extensive threat defense capabilities, Deep Security helps financial services organizations streamline compliance efforts, simplify security management and deliver evidence to auditors documenting continuous protection from vulnerabilities, detected attacks and policy compliance status for workloads dealing with regulated data no matter where they reside.

Ingram Micro's Trend Micro market development experts are ready to help you develop security solutions for your SMB customers. Call (800) 456-8000, ext. 67485 or email trendmicromd@ingrammicro.com for support.