CHOICE CYBERSECURITY

Financial Services

Security & Compliance Resource Guide

Table of Contents

U.S. Securities and Exchange Commission (SEC) 2

FINRA Compliance 5

FFIEC Compliance 8

Financial Services Security and Compliance Needs Analysis 10

U.S. Securities and Exchange Commission (SEC)

What is it?

The Securities and Exchange Commission (SEC) is a U.S. government agency that prevents fraud and international deception by overseeing securities transactions, activities of financial professionals and mutual fund trading. The SEC provides cybersecurity guidance to help broker-dealers, investment advisers, investment companies, exchanges, and other market participants protect their customers from cyber threats.

The SEC has four major divisions.

- The Division of Corporation Finance ensures corporate disclosure of important information to the investing public.
- The Division of Trading and Markets ensures fairness, order and efficiency in market activities.
- The Division of Investment Management helps protect investors and encourages capital formation through oversight and regulation of the investment management industry.
- The Division of Enforcement investigates securities law violations and initiates civil and criminal actions.

Division of Investment Management

The Division of Investment Management (Division) works to protect investors, promote informed investment decisions and facilitate appropriate innovation in investment products and services through regulating the asset management industry. The Division is responsible for the Commission's regulation of investment companies, variable insurance products, and federally registered investment advisers. Types of investment companies include mutual funds, closed-end funds, business development companies, unit investment trusts, and exchange-traded funds.

The Division carries out its mission by focusing primarily on guidance, disclosure, rulemaking, and risk monitoring and analysis. Its work is generally performed by the following offices:

- Guidance – Chief Counsel's Office
- Disclosure – Disclosure Review and Accounting Office
- Rulemaking – Rulemaking Office
- Risk Monitoring – Risk and Examinations Office

Risk Monitoring

The Division's Risk and Examinations Office (REO) monitors trends in the asset management industry and carries out the Division's inspection and examination program. REO pursues its mission by: (1) managing, monitoring, and analyzing the industry data the Division gathers; (2) providing ongoing financial analysis of the asset management industry; (3) gathering and analyzing operational information directly from participants in the asset management industry, including in particular the risk-taking activities of investment advisers and investment companies; and (4) otherwise maintaining industry knowledge and technical expertise to provide other analyses that may support the Division's activities.

SEC Audits

While the Securities and Exchange Commission does not, in and of themselves, have a compliance requirement, an SEC audit looks closely into whether organizations are adhering to the compliances that are required by other laws, such as SOX, FISMA, etc.

In order to maintain a high level of confidence in passing an SEC audit, organizations must ensure that they have a written Information Security Policy and proof that they have implemented and are adhering to the policy, including regular risk assessments.

Overview of SEC Cybersecurity Guidance

The Division has identified the cybersecurity of registered investment companies ("funds") and registered investment advisors ("advisers") as an important issue. Both parties need to protect confidential and sensitive information related to these activities from third parties. Cyber attacks on all different financial service firms highlight the need for films to review their security measures.

Risk Assessment

There are a number of measures that funds and advisers may wish to consider in addressing cybersecurity risks including:

- Conducting a periodic assessment of:
    - Nature, sensitivity and location of information (collected and stored)
    - Internal/ external cybersecurity threats and vulnerability of the firm
    - Security controls and processes currently in place
    - The impact should the information or technology become compromised
    - The effectiveness of the governance structure for the management of cybersecurity risk
- Creating a strategy designed to prevent, detect and respond to cybersecurity threats and respond to cybersecurity threats which should include:
    - Access control to various systems and data
    - Data encryption
    - Protection against the loss and damage of sensitive data
    - Data backup and retrieval

- Implementing the strategy through written policies and procedures and training that provides guidance and training to all employees

SEC Resources

- SEC Cybersecurity Guidance

FINRA Compliance

What is it?

FINRA is the Financial Industry Regulatory Authority, an organization that provides oversight to brokerage firms and exchange markets. FINRA was established in 2007 by the merging of the National Association of Securities Dealers and the regulatory arm of the New York Stock Exchange.

Who oversees it?

The Securities and Exchange Commission.

Who does it apply to?

Organizations involved in the sale of financial securities.

How does it impact IT professionals?

Email archiving and retention plays a large part in the SEC and FINRA rule requirements. IT professionals may be called upon to implement and maintain an email archiving solution for clients who are subject to SEC and FINRA rules.

What do your clients need to be FINRA compliant?

FINRA 3110

Each firm must preserve accounts, records, and correspondence in adherence to applicable laws, SEC rules, and FINRA rules and regulations.

FINRA 3010

Each firm must maintain a system to supervise transactions and correspondence with their users. Firms should establish a supervisory system with written procedures that govern the regular review of incoming and outgoing electronic correspondence.

SEC 17a-3-4

Each firm must maintain a written, enforceable data retention policy, including searchable indexes of data stored. Data must furthermore by securely stored offsite in tamper-proof storage media.

What are the dangers of not being FINRA compliant?

- Initial fines of up to $100,000
- Additional monetary sanctions from $5000 to several millions of dollars
- Suspension
- Individual ban
- Firm expulsion

Event and Audit Log Retention Requirements

In order to maintain FINRA compliance, event and audit logs must be retained for a period of six years. However, the SEC recommends keeping event and audit logs, as well as client files, indefinitely.

FINRA Compliance Services at a Glance

In order to maintain compliance with the FINRA rules and regulations, firms are required to maintain a searchable record of all electronic correspondence as well as a comprehensive Information Security Policy that proves that all applicable steps have been taken to protect sensitive data on the network.

MSPs can best assist their clients in achieving FINRA compliance by offering a comprehensive email archiving solution and developing a tailored Information Security Policy for their clients and assisting them in implementing the written policy.

FINRA Cyber Security Risk Assessment

Overview

Firms should conduct regular assessments to identify cybersecurity risks associated with firm assets and vendors. Firms should establish and implement frameworks to:

- Identify and maintain an inventory of assets authorized to access the network and critical assets
- Conduct comprehensive risk assessments to include:
    - An assessment of external and internal threats and asset vulnerabilities
    - Recommendations to remediations to remediate identified risks which can be one of the following:
        - Preventive - prevents harm from taking place in the first place
        - Detective - identify potential threats that may have occurred

  - Corrective - restore a system back to the state prior to the threat
  - Predictive - predict the detrimental event happening

A cybersecurity risk assessment is a systematic process firms complete to identify and analyze potential dangers or risks. Such risks could include the compromise of confidential information, misuse of customer funds or securities.

Framework

Both NIST framework and SANS CIS Top 20 Critical Security Controls identify inventories and the NIST framework also underscores the importance of identifying critical assets. An effective inventory process will define measures of importance. Firms take different measures to begin the inventory process including:

- Completing a questionnaire where they will identify all assets
- Setting a critical or risk threshold and ask the business unit to identify assets that meet or exceed that threshold
- A team provides a list of assets that the business unit validates

The NIST framework identifies 6 sets of risk assessment activities and outcomes:

- Identify and document asset vulnerabilities
- Review threat and vulnerability information
- Identify and document internal and external threats
- Identify potential business impacts and likelihoods
- Use threats, vulnerabilities, likelihoods and impacts to determine risk
- Identify and prioritize risk responses

Organizational Structure

Larger firms sometimes have the option to complete risk assessment in-house, while smaller firms tend to outsource the risk assessment process to a vendor. FINRA states that it is important that all firms, despite their size, have a defined escalation process to address risks identified as not appropriately mitigated. The more significant the risk, the higher the level of management approval required to accept that risk.

FINRA RESOURCES

- FINRA Sanctions Guidelines
- FINRA Report on Cyber Security Practices
- FINRA SMB Cyber Security Checklist

FFIEC Compliance

What is it?

The Federal Financial Institutions Examination Council (FFIEC) is an interagency body established to define and enforce uniform principles, standards, and report forms for financial institutions.

Who oversees it?

A Board of Governors comprised of members of the Federal Reserve Board, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currents, and the Consumer Financial Protection Bureau.

Who does it apply to?

National banks and their subsidiaries, state banks, bank holding companies, savings and loan holding companies, branches and agencies of foreign banking organizations, and credit unions.

How does it impact IT professionals?

In June 2013, the FFIEC created the Cybersecurity and Critical Infrastructure Working Group to identify gaps in protection and strengthen the oversight of cybersecurity readiness. MSPs may be called upon to help their financial services clients built a robust security infrastructure to protect sensitive financial data and customer records.

What do your clients need to be FFIEC compliant?

The FFIEC can audit a financial institution at any time. In order to pass an FFIEC audit, the financial institution must have a documented Information Security Policy in place with proof of a recent Security Risk Assessment. In addition to these requirements, financial organizations must meet the regulatory requirements of any organizations (such as the FRB, FDIC, etc.) with direct oversight of the institution.

What are the dangers of not being FFIEC compliant?

The FFIEC does not impose fines and sanction directly. However, failure to pass an FFIEC audit can result in fines and sanctions from the Federal Reserve Board, Federal Deposit Insurance Corporation, and the National Credit Union Administration. Fines can range from $10,000 to $1,000,000 per incident, with sanctions up to and including dissolving the offending institution.

FFIEC Compliance Services at a Glance

MSPs can help their clients by implementing and maintaining a robust Information Security Policy and providing support services in the form of regular risk assessments and vulnerability audits. Being able to prove that an institution is proactive regarding their information security will go a long way toward meeting the requirements of an FFIEC audit.

What is the FFIEC Cybersecurity Assessment?

The FFIEC Cybersecurity Assessment is designed to help organizations identify their cybersecurity risks. This process is intended to complement, not replace, an organization's risk management process and cybersecurity program.

- Assesses the complexity of an organization's operating environment, including:
  - Technologies and Connection Types
  - Delivery Channels
  - Online/Mobile Products and Technology Services
  - Organizational Characteristics
  - External Threats
- Assesses an organization's current practices and initiatives focusing on:
  - Risk Management and Oversight
  - Threat Intelligence and Collaboration
  - Cybersecurity Controls
  - External Dependency Management
  - Cyber Incident Management and Resilience
- Assist FFIEC member agencies in:
  - Making risk-informed decisions to identify and prioritize actions
  - Enhancing the effectiveness of cybersecurity-related initiatives
  - Identifying actions that can strengthen their overall level of preparedness and ability to address the evolving and increasing cybersecurity threats

FFIEC Resources

- FFIEC Cybersecurity Assessment Tool
- FFIEC Cybersecurity Assessment Tool FAQs
- IT Booklets
  - Audit
  - Business Continuity Planning
  - Information Security
  - IT Management
  - Outsourcing Technology Services
  - Additional Booklets

Financial Services Security and Compliance Needs Analysis

Needs Analysis Below are 4 areas to discuss with financial clients when analyzing specific security needs. Utilize these questions and answers to create the Risk Assessment proposal.

Financial Compliance

1. Do you have any compliance requirements?
2. Do you report to the SEC, FINRA etc?
3. Have you ever been audited? Were you ready?
4. Are you familiar with state PII laws?
5. Do you take credit cards? If so, are you PCI compliant?
6. How many credit cards do you process per year?
7. What is the credit card process?
8. Who in the company is responsible for compliance?
9. Have you ever had an audit or fine?
10. Do you know anyone who has had a breach?
11. Do you have a best practices or compliance structured framework in place? If so, what controls do you follow?
12. Has your staff had any specific compliance training?
13. How do you handle compliance management?
14. Do you capture and review logs?

General Business

1. Do you store sensitive data?
2. How important is your data?
3. How much is your data worth?
4. Do you know how much sensitive data you store?
5. Who is the asset owner and responsible for your data?
6. How many states do you operate in?
7. How are backups done? Onsite? Offsite?
8. Do you have an incident response plan?
9. Have you ever had a risk assessment?
10. Have you ever had a vulnerability scan or penetration test?
11. Do you have a structured password policy? Where are passwords stored?
12. Do your users have remote access? How do they connect?
13. Do you require any of your clients to have security in place?
14. Do any of your clients require you to have any security or compliances in place?
15. Do you have Cybersecurity Insurance? Ever had a claim?

16. How many servers, workstations and laptops are in place?
17. How do you handle mobile devices?
18. Do you have an employee handbook with security policies?
19. Has your staff had security awareness training?
20. Do you know your potential collateral damage in the event of a breach?

Security

1. Who is responsible for security?
2. Have you ever had a virus or infected system?
3. Have you ever lost any files?
4. Have you ever had a breach?
5. Has a machine ever been lost or stolen?
6. Have you ever had a server crash?
7. What is the longest period of downtime you have experienced?
8. Are you concerned about a breach?
9. Any vendors asking you for security requirements?
10. What would be the impact to your business of a security breach?
11. Do you have email or file encryption?

Workflow

Data in Motion

1. Do you send sensitive data via email?
2. Do you transfer large files?
3. Do you receive sensitive data from outside sources? If so, do you save it locally?
4. Do you send wire transfers?
5. Do you upload and download files from any cloud systems?

Data at Rest

1. Where is sensitive data stored?
2. What is your retention policy for files?
3. What is your retention policy for email?

Vendors

1. How many vendors do you work with? How many cloud vendors?
2. Do you store sensitive data in the cloud?
3. Do any vendors have access to your systems?
4. Do you send sensitive data to your vendors?
5. Do your vendors have any of your sensitive client data?
6. Do your vendors send you sensitive data?
7. Do any of your vendors require you to have any security or compliances in place?