The financial industries are being increasingly targeted by cyber thieves. This paper focuses on the latest cyber-security requirements for financial institutions with brokers-dealers, investment advisors, and investment funds that are regulated by Financial Industry Regulatory Authority (FINRA) and the Securities and Exchange Commission (SEC).

THE REGULATORS

The Financial Industry Regulatory Authority (FINRA) is a self-regulatory non-governmental organization that regulates member brokerage firms and exchange markets. FINRA’s primary mission is to protect investors. FINRA will utilize both examinations and targeted investigations to evaluate the adequacy of firm policies and information technology systems to protect sensitive investor information.

FINRA’s stated goal of protecting investors contributes to a continued focus on cyber-security and data integrity. FINRA has noted that the increased frequency and sophistication of cyber-attacks against the industry is a persistent and ever-changing threat. FINRA’s focus on cyber-security is also driven by the sensitivity of investor data in financial transactions. FINRA has committed to diligently monitor the information security policies and procedures of member firms. The industry’s heavy reliance on computer-based client information and financial systems make it clear that this aspect of business conduct needs to be closely monitored.

Through examinations and targeted investigations, FINRA will target any firm whose information security and customer data controls are lacking. The government agency which acts as the ultimate regulator, including FINRA, is the Securities and Exchange Commission (SEC).

RECENT EXAM FOCUS

In 2013, FINRA’s examiners focused on the integrity of firms’ policies, procedures and controls to protect sensitive investor data and significant gaps that could lead to investigations or enforcement action.

In 2014, FINRA will increase examinations and targeted investigations of firms’ infrastructure and the safety and security of sensitive investor data. Firms are well-advised to ensure that their data security systems and procedures are up-to-date, since the financial and reputational impact of adverse examination findings or enforcement actions can be devastating.

On January 2, 2014, FINRA issued a statement, which said, “Cyber-security remains a priority for FINRA in 2014 given the ongoing cyber-issues reported across the financial services industry. In recent years, many of the nation’s largest financial institutions were targeted for disruptions through a range of different types of attacks. The frequency and sophistication of these attacks appears to be increasing. In light of this ongoing threat, FINRA continues to be concerned about the integrity of firms’ infrastructure and the safety and security of sensitive customer data. Our primary focus is the integrity of firms’ policies, procedures and controls to protect sensitive customer data. FINRA’s evaluation of such controls may take the form of examinations and targeted investigations.”

Additionally, FINRA issued a regulatory guidance notice of “targeted examinations” of investment firms to review their approaches to managing cyber-security threats. These targeted exams, better known as “sweeps” are to gather information, carry out investigations, and assist in pinpointing regulatory response to emerging issues. Following are highlights of what will be assessed during the FINRA examination sweeps.
Examination Goals:
• Better understand the types of threats firms face
• Increase understanding of firms’ risk appetite, exposure and major areas of vulnerabilities in their IT systems
• Better understand firms’ approaches to managing these threats, including through risk assessment processes, IT protocols, application management practices and supervision
• Share observations and findings with other firms

Assessment Areas:
• Approach to information technology risk assessment
• Business continuity plans in case of a cyber-attack
• Processes for obtaining and sharing information about cyber-security threats
• Organizational structures and reporting lines
• Concerns and threats
• Assessment of the impact of cyber-attacks on the firm over the past 12 months
• Approach to handling distributed denial of service attacks
• Security (cyber & information) training programs
• Insurance coverage for cyber-security related events
• Contractual arrangements with third-party service providers (who have access)

CYBER-ATTACK EXAMPLES
A common scenario of a breach involves individuals who hack into the private email accounts of FINRA members’ customers, gaining access to the clients’ correspondence with the firms. Posing as the customer, the hackers then tell the firm there has been an emergency and seek to move thousands of dollars worth of cash or securities. Because everything looks legitimate from the firm’s perspective, the company wires out the money into an account that the customer had never used before. Firms wire money to hackers either because the customer validation procedures are inadequate or because the firm employees are in a hurry to assist the client.

As an example of what cost an attack could have on an organization, in April 2010 FINRA fined a financial services company $375,000 for its failure to protect confidential customer information by allowing an international crime group to improperly access and hack the confidential information of approximately 192,000 customers. FINRA found that prior to January 2008, the company did not employ adequate safeguards to protect the security and confidentiality of customer records and information stored in a database housed on a computer Web server with a constant open Internet connection. The unprotected information included customer account numbers, social security numbers, names, addresses, dates of birth and other confidential data. Furthermore, the firm’s procedures for protecting that information were deficient in that the database was not encrypted and the firm never activated a password, thereby leaving the default blank password in place.

The hacker used “SQL injection,” an attack in which computer code is repeatedly inserted into a Web page for the purpose of extracting information from a database. The hacker was able to access and download customers’ confidential information. While these attacks were visible on Web server logs, the firm failed to review those logs. The breach was discovered through an email that was sent by the hacker on Jan. 16, 2008, blackmailing the firm.

In addition to the FINRA fine, the firm offered affected customers a subscription to a credit-monitoring service for two years at a cost of $1.3 million.

THE REGULATION
SEC Final Rule 30(a) on Consumer Financial Information (Regulation S-P)
Effective November 13, 2000 and mandatory as of July 1, 2001, the SEC adopted the privacy rules promulgated under section 504 of the Gramm-
Leach-Bliley Act (GLBA). Under the GLBA, a financial institution must establish appropriate standards to protect customer/investor information. Otherwise known as the “Safeguards Rule” SEC 17 CFR 248.30, this requires broker-dealers (investment funds and advisors) to maintain reasonably designed policies and procedures to protect the non-public information (NPI) of their customers from security threats and unauthorized access. The SEC can allege a violation of the Safeguards Rule by not putting in place policies and procedures to address the transfer and protection of its customers’ information, even for terminated employees.

**FINRA Customer Information Protection Guidance**

Protection of financial and personal customer information is a key responsibility and obligation of FINRA member firms. This includes protecting against any anticipated threats or hazards to the security or integrity of customer records and information and against unauthorized access to or use of customer records or information. This is especially true for firms that offer online, Web-based access to platforms. Firms must understand and address the potential risks of account intrusions, whereby an unauthorized person gains access to a customer account and either steals available assets or misuses the account. Intrusions are generally accomplished through the theft of the login credentials of a customer or firm employee. Since this type of illicit activity can harm both the investor and market integrity, it is essential that firms use reasonable measures to protect customer information and assets.

**TYPICAL VIOLATION AREAS**

While a single sign-on has been determined to be the biggest problem, the following items listed below make up the majority of security weaknesses, as determined by FINRA’s 2013 sweep exams.

- **Policies and Procedures**
  - Failure to adopt written procedures setting forth an information security program designed to respond to intrusions
  - Failure to establish procedures mandating that employees install anti-virus software and other protection on their computers
  - Failure to implement procedures for the encryption of laptops or data stored on laptops

- **Encryption, Password Protection, And Anti-Virus And Security Software**
  - Failure to use a properly configured computer firewall
  - Failure to audit employee computers to confirm the installation of security software
  - Failure to monitor for potential or actual breaches
  - Failure to enforce the mandated use of strong passwords through validation or periodic password changes and a forced password expiration
  - Failures to employ effective usernames and passwords, or to place controls and procedures on the use and dissemination of the usernames and passwords
  - Failure to review web server logs revealing intrusions
  - Failure to implement appropriate encryption measures
  - Allowing employees to share computer sign-on credentials to access files which contained confidential customer information
  - Storing a database containing customer information on a computer with a persistently open Internet connection which left the information in the database exposed to the internet

- **Training, Audits and Consultant Recommendations**
  - Failure to perform sufficiently broad periodic audits to protect customer records and other sensitive information from unauthorized access
  - Failure of a firm to carry out the security recommendations of independent auditors and outside security consultants for an intrusion detection system
- Failure to provide adequate training to employees regarding customer breaches, leading to the failure of certain employees to recognize that an unauthorized customer account data breach had occurred and that the breach had to be reported to the firm’s compliance department and privacy officer

• Customer Notifications
  - Failure to provide customers with an opt-out notice prior to disclosing their information to the nonaffiliated third party
  - Sending misleading notification letters to affected customers and advisors

WHAT TO DO NEXT

Important next steps would be to ensure your organization has policies and procedures in place (process, methodology and frequency) for protecting investor data, checking on the latest cyber-threats in the news, monitoring for threats, an incident response plan, and proactive risk assessment reviews.

It is highly recommended that an annual FINRA Information Security audit be conducted to ensure that all aspects of FINRA and SEC safeguarding requirements are in place.

To get started, obtain and complete FINRA’s Examination Sweep Survey Questionnaire or Risk Control Assessment (RCA) Survey. These documents can be downloaded from the FINRA website.

For more information, please contact:
Glenn Hoffman
Managing Director, Technology Risk Management
203.803.7345 or ghoffman@accumepartners.com

References:
FINRA - Financial Industry Regulatory Authority:
http://www.finra.org/

ABOUT ACCUME PARTNERS

Accume Partners offers a suite of internal audit, compliance, technology risk management and enterprise risk management services that reflects a broad range of expertise and business solutions across multiple industries. Accume is a trusted partner in helping clients navigate the landscape of corporate responsibility, regulatory and financial accountability. Accume offers customized solutions for meeting internal audit, compliance and risk requirements, and a myriad of governance issues by delivering comprehensive, practical support to management.

Copyright 2014 Accume Partners, All rights reserved.