WINSTON & STRAWN LLP

BLOG

FINRA Notifies Members of Cyber-Security Sweeps

FEBRUARY 26, 2014

The Financial Industry Regulatory Authority, Inc. (FINRA) recently notified its members that it is conducting targeted exams, known as sweeps, that are designed to assess member's approaches to managing cyber-security threats. A copy of FINRA's notice is available here. FINRA's assessment is designed to address a wide variety of concerns, including: approaches to information technology risk assessment; business continuity plans in case of a cyber-attack; approaches to handling distributed denial of service attacks; training programs; insurance coverage for cyber-security-related events; and contractual arrangements with third-party service providers. FINRA's sweep follows on the heels of a number of statements over the last several years by the Securities and Exchange Commission (SEC) and FINRA highlighting issues raised by cyber-security for broker-dealers. While the SEC and FINRA are most focused on the potential impact posed by cyber-security on customers, broker-dealers should understand that although the risk posed by cyber-security may be greatest for clearing and carrying firms, cyber-security should also be of concern even to introducing broker-dealers. Cyber-security concerns extend to employee and workplace privacy concerns, the need to protect individuals' financial data, whether employees or customers, and the need to comply with a myriad of state and federal privacy laws including breach notification laws. If they occur, data breaches can cause significant reputational issues and lead to inquiries, investigations and remediation efforts that can be expensive, time consuming and intrusive, as well as significant fines and litigation expenses.

Tip: Addressing cyber-security concerns requires inventorying risks and developing and implementing a plan to address the identified risks. This plan should also address training, monitoring, internal reporting and the need for periodic testing. Plans must also be kept current in the face of changes in practices or technology and should be updated periodically to reflect the changing risk environment. Firms should also map out responsibilities so that they are able to respond quickly and efficiently should a breach or suspected breach occur.

1 Min Read

Related Locations

Chicago

Related Topics

Data Breach

Related Capabilities

Privacy & Data Security

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.