AN ALERT FROM THE BDO FINANCIAL SERVICES PRACTICE

ASSET MANAGEMENT INSIGHTS

SECURITIES INDUSTRY SHOULD TIGHTEN CYBERSECURITY CONTROLS AND PROCEDURES AS REGULATORY PRESSURE INTENSIFIES

Financial regulators are tightening their grip on cybersecurity issues. In early January, the Financial Industry Regulatory Authority (FINRA) addressed the measures it would take this year to review firms' cybersecurity risk management practices.

This follows the SEC's Office of Compliance Inspections and Examinations (OCIE) rollout of a second round of examinations on cyber-related controls and procedures in the securities industry. In its September 2015 Risk Alert, the OCIE announced an update to its Cybersecurity Examination Initiative, identifying a number of critical areas it will test to assess cybersecurity preparedness, including the ability to protect broker-dealer customer and investment advisor client information.

In March, the SEC announced the creation of the Office of Risk and Strategy within the OCIE. The new office, led by Peter B. Driscoll, will "consolidate and streamline the OCIE's risk assessment, market surveillance, and quantitative analysis teams and provide operational risk management and organizational strategy for OCIE."

Summary

FINRA's annual Regulatory and Examination Priorities Letter, issued in January 2016, stresses concerns about shortcomings in securities firms' technology systems and cybersecurity defenses. The supervision and risk management of firms' cybersecurity, technology management, and data quality and governance will be closely examined in 2016. FINRA's letter calls attention to a number of specific problem areas, including:

- The ability to protect confidentiality, integrity and availability of sensitive customer and other information, including compliance with SEC Regulation S-P and Securities Exchange Act Rule 17a-4(f).
- High-frequency and proprietary trading firms' ability to protect their systems from unauthorized access that could be used to affect the market.
- Supervision of back office and vendor system changes; change management practices for algorithms will be closely scrutinized, as will changes from legacy to new compliance systems.
- Data governance, quality controls and reporting practices to ensure the accuracy, completeness, consistency and timeliness of data reported to firm management and to firms' surveillance and supervisory systems.

FINRA's cybersecurity focus aligns neatly with efforts underway by the SEC. In April 2014, the OCIE initiated a series of examinations on cybersecurity risks in the securities industry, which identified a variety of cyber-related legal, regulatory and compliance issues published in a February 2015 report. Cybersecurity compliance and controls became the focus of OCIE's 2015 Examination Priorities, prompting an announcement in September 2015 that a new round of examinations would be conducted around firm cybersecurity procedures and controls. Shortly thereafter, the SEC released its first enforcement action

BDO'S FINANCIAL SERVICES PRACTICE

BDO's Financial Services Practice provides assurance, tax and advisory services to asset management entities, primarily Hedge Funds, Private Equity Funds, Broker Dealers and Mutual Funds. The practice services over 600 advisors nationwide with funds ranging from start-up funds to those with billions under management.

ABOUT BDO USA

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through 63 offices and more than 450 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,408 offices in 154 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Read more ▶

against a securities firm for inadequate cyber safeguards, charging the investment adviser with a failure to "establish the required cybersecurity policies and procedures in advance of a breach."

Further, the establishment of the new Office of Risk and Strategy and appointment of Peter Driscoll in the OCIE signals an additional layer of oversight and scrutiny on the OCIE's priorities related to cybersecurity specifically and risk broadly. ThinkAdvisor reports public comments from Driscoll suggesting that funds and fund advisors would "continue to be a big focus" for the OCIE in 2016, and the "focus on hedge funds will zero in on such areas as portfolio management trading and back-office operations."

While more guidance is expected soon, it has previously been announced that the OCIE will be focusing its review on cyber-related policies, procedures and practices in these key areas:

- Governance and risk assessment
- Access rights and controls
- Data loss prevention
- Vendor management
- Training
- Incident response

BDO Insights

Regulators expect that these reviews and additional regulatory oversight will prompt securities firms to closely examine their own vulnerabilities and practices, and find ways to tighten existing gaps. As the nature of cyber breaches continues to evolve at a rapid pace, it would behoove firms to renew their focus on information governance and access controls, and implement ongoing defensive measures that continuously scan for new weaknesses and threats. FINRA clearly stated its intentions to assess the abilities of high frequency and proprietary trading firms to protect data, so organizations leveraging automated trading platforms should be especially vigilant. Similarly, the creation of the Office and Risk Strategy group suggests that OCIE is stepping up its cybersecurity enforcement, with an eye on hedge funds in particular.

Also of note, included in the sample list of information that the OCIE may review in conducting examinations of registered entities are the board's minutes and briefings regarding cybersecurity matters. While the guidance is not explicit, it implies an expectation that the board is not only informed, but also playing an active role in the firm's cybersecurity strategy. FINRA also announced its plans to review reporting practices to firm management, as well as to firms' surveillance and supervisory systems, focusing on the accuracy, completeness, consistency and timeliness of the reports. We will likely see additional guidance from regulators on board oversight and reporting in the future, but in the interim, the board should request cyber updates at regular intervals and work with management, IT and internal auditors to get educated and ask the right strategic questions.

While firms should take steps to protect their data and detect cyber attacks early on, no defense is impenetrable. Securities firms are expected to have an incident response plan in place that enables them to rapidly detect, respond and mitigate the potential consequences of a future breach.

Financial services firms are well-advised to seek assistance from consultants and technology specialists experienced in developing risk management frameworks and strategies to navigate complex security and compliance issues. BDO has deep experience in conducting cybersecurity risk assessments, cyber risk management strategy and program design, security architecture and transformation, incident response planning and execution, digital forensics and cyber investigations, as well as cyber insurance claim preparation and coverage adequacy evaluation.

For more information about how securities firms can improve their cybersecurity preparedness, please contact:

SHAHRYAR SHAGHAGHI
National Leader, Technology Advisory Services & Head of International BDO Cybersecurity
sshaghaghi@bdo.com

KEITH MCGOWAN
Asset Management & Broker Dealers National Practice Leader and Assurance Partner
kmcgowan@bdo.com

TIM MOHR
BDO Consulting Financial Services Advisory
National Practice Leader
tmohr@bdo.com