CLIENT ALERT

Cybersecurity Threats: Regulators Put Broker-Dealers and Investment Advisers on Notice

Feb.09.2015

On February 3, 2015, the U.S. Securities and Exchange Commission (SEC) and The Financial Industry Regulatory Authority (FINRA) simultaneously published information addressing cybersecurity. Cybersecurity has been a theme of increasing importance. Broker-dealers and investment advisers should be on notice that regulators expect them to maintain up-to-date policies and tailored procedures to isolate cybersecurity threats.

The SEC issued two publications addressing cybersecurity at brokerage and advisory firms addressed to the firms and to investors, which can be found here and here. FINRA published both a comprehensive report that details practices that brokerage firms can use to strengthen their cybersecurity efforts and also issued an investor alert to customers, which can be found here.

SEC Cybersecurity Alert

The first SEC publication is a Risk Alert from the SEC's Office of Compliance Inspections and Examinations (OCIE). It contains observations based on examinations of more than 100 broker-dealers and investment advisers. The examinations focused on how these firms:

- Identify cybersecurity risks
- Establish cybersecurity policies, procedures, and oversight processes
- Protect their networks and information
- Identify and address risks associated with remote access to client information, funds transfer requests, and third-party vendors
- Detect unauthorized activity

The SEC Risk Alert provided the following findings:

- The vast majority of examined broker-dealers and advisers have adopted written information security policies, regularly perform risk assessments, and conducted technology catalogues or maps.

- A majority of the broker-dealers and advisers stated that they have experienced cyber-attacks directly or through one or more of their vendors, including receiving fraudulent emails seeking to transfer client funds that have resulted in loss.

- Most examined firms report using some form of encryption technology.

- More than half of examined broker-dealers, but less than a third of examined advisers, have designated a Chief Information Security Officer (CISO).

- A significantly higher percentage of examined broker-dealers than advisers report maintaining cybersecurity insurance.

- Broker-dealers appear to be a step ahead of advisers in terms of cybersecurity risk assessments and maintaining appropriate policies and procedures. Advisers should expect heightened attention by OCIE in upcoming examinations.

The second SEC publication is an Investor Bulletin issued by the SEC's Office of Investor Education and Advocacy (OIEA). It provides core tips to help investors safeguard their online investment accounts, including advising investors to pick a "strong" password, use two-step verification, and exercise caution when using public networks and wireless connections.

The FINRA *Report on Cybersecurity Practices* draws in part from the results of FINRA's recent targeted examination (sweep) of a cross-section of firms. The sweep, conducted in 2014, focused on the types of threats firms face, areas of vulnerabilities in their systems and firms' approaches to managing these threats. The FINRA report not only contains valuable advice for firms to assess risks and establish their cybersecurity programs, but also sets forth key issues that are on FINRA's radar for exams and enforcement actions, including:

- Focus on smaller firms, which may lag behind in development of cybersecurity programs
- The importance of encryption and adequate password protection
- Using metrics to assess vulnerability and responding to red flags indicating intrusion attempts
- Adequacy of employee training
- Limiting employee access to sensitive databases
- The importance of telephonic verification of requests for wire transfers
- FINRA's expectation that firms will reimburse customers for losses
- The necessity to monitor customer account activity

FINRA Cybersecurity Alert

FINRA also issued an Investor Alert called *Cybersecurity and Your Brokerage Firm*, which encourages investors to understand their firm's cybersecurity policies. FINRA's new Investor Alert includes a series of questions investors can ask to help them better understand their firm's cybersecurity activities and policies, as well as practical advice to help investors safeguard their brokerage accounts and personal financial information.

Broker-dealers are increasingly exposed to cybersecurity risks. FINRA's report reveals that the top three threats are:

- Hackers penetrating firm systems
- Insiders compromising firm or client data
- Operational risks

The FINRA report found that online brokerage firms and retail brokerages are more likely to list hackers as their top-priority risk while firms that engage in algorithmic trading were more likely to consider insider risks potentially more damaging. Large investment banks or broker-dealers typically ranked risks from nation states or hacktivist groups more highly than other firms.

Takeaways

Based on the SEC and FINRA guidance, we suggest the following as best practices in addressing cybersecurity:

- **Strong and accountable leadership**: Companies should establish a clear point of contact for cybersecurity (*e.g.*, Chief Information Security Officer) that works with other key constituencies across the firm (*e.g.*, personnel from the legal and operations departments).
- **Risk Management Process**: A mature risk management process helps to both identify risks and mitigate them. Such a process should include conducting regular network security assessments and similar tests and then ensuring that senior leadership review and understand the results. The organization should also assess its ability to respond to everyday threats, such as spear phishing attacks and other forms of social engineering. The fact that broker-dealers seem a step ahead of investment advisers in cybersecurity risk management should put advisers on notice that OCIE can be expected to devote additional attention to cybersecurity in upcoming examinations.
- **Governance**: Key personnel (*e.g.*, individuals from management, audit, communications, and legal) should have clearly defined roles and responsibilities and should meet to help ensure there are clear communication channels.
- **Incident Response Plan**: Risk can be significantly mitigated by developing, implementing, and testing an Incident Response Plan. The plan should identify key terms (*e.g*, how an "Incident" is defined), describe roles and responsibilities, detail the escalation processes, and contain a toolkit of prepared documents (*e.g.*, template notification letters). It is also helpful to arrange in advance for a technical consulting firm to be available for immediate response efforts following an incident.
- **Suspicious Activity Reports**: The SEC noted that almost two-thirds of broker-dealers that received fraudulent emails reported the emails to the Financial Crimes Enforcement Network (FinCEN by filing a Suspicious Activity Report (SAR). In many instances, SARs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations and other criminal cases. FinCEN requires a SAR to be filed by a financial institution when the financial institution suspects insider abuse by an employee; violations of law aggregating over $5,000 where a subject can be identified; violations of law aggregating over $25,000 regardless of a potential subject; transactions aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act; computer intrusion; or when a financial institution knows that a customer is operating as an unlicensed money services business.
- **Vendors**: Vendors are often the weak link in the security chain. Broker-dealers should manage vendor risk by undertaking robust due diligence efforts throughout the vendor lifecycle, including proper vetting, strong contract terms (*e.g.*, broad indemnity clauses), and limiting vendor access to sensitive information and systems.
- **Training**: Organizations should develop a robust training program that includes baseline training for all employees as well as enhanced training for individuals that pose higher risks (*e.g.*, senior management and IT staff).
- **Information Sharing**: Organizations can benefit from sharing information regarding cyber threats and mitigation activities with both industry groups (*e.g.*, Information Sharing and Analysis Organizations (ISAO) or Information Sharing and Analysis Centers (ISAC)), as well as with government partners. Such sharing makes it more difficult for adversaries to exploit vulnerabilities.

Additionally, wherever a firm is in its cybersecurity efforts, we urge our clients to review both the SEC and FINRA reports. Even advisory firms not subject to FINRA jurisdiction would benefit from the FINRA guidance and resources.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com