Published on *The National Law Review* https://natlawreview.com

FINRA Cybersecurity Report Highlights Risks, Best Practices - Financial Industry Regulatory Authority

Article By:

David A. Picon

Edward Canter

On February 3, 2015, the ***Financial Industry Regulatory Authority ("FINRA")*** issued its *Report on Cybersecurity Practices*. Reinforcing FINRA's emphasis on protecting investor information, the report discusses the results of a recent industry-wide cybersecurity examination and presents a list of principles and best practices to guide the industry's cybersecurity efforts going forward.

2014 Cybersecurity Examination

Last year, FINRA conducted a targeted examination of certain firms in the financial services industry. The examination sought information about various cybersecurity threats and firms' particular vulnerabilities. The examination gathered information about firms' approaches to managing these threats.

The report identifies a number of diverse *"threat actors,"* including "***cybercriminals whose objective may be to steal money or information for commercial gain, nation states that may acquire information to advance national objectives***, and hacktivists whose objectives may be to disrupt and embarrass an entity." The report emphasizes that insiders can pose significant cybersecurity threats.

The canvassed firms expressed particular concern about the risk of hackers penetrating firm systems, insiders compromising firm or client data, and certain operational risks. The perceived risk of these threats varied by firm, with "online brokerage firms and retail brokerages . . . more likely to rank the risk of hackers as their top priority risk" and "[f]irms that engage in algorithmic trading . . . more likely to rank insider risks more highly." Notably, the examination found that "large investment banks or broker-dealers typically ranked risks from nation states or hacktivist groups more highly than other firms."

Principles and Best Practices

To counter the risk of cybersecurity threats, FINRA emphasizes the importance of pairing a strong governance framework with regular cybersecurity risk assessments and appropriate technical

controls. FINRA suggests that senior management and the board of directors should take an active role addressing cybersecurity issues, as firms with an actively engaged board "had a strong positive impact in focusing attention on, and making resources available for, cybersecurity."

The report identifies vendors and employees as significant sources of cybersecurity risk and recommends that firms adopt additional safeguards. Noting that data may be put at risk if a vendor's systems come under attack, FINRA recommends that firms conduct vendor due diligence before entering into service agreements. FINRA also emphasizes the importance of strong privacy and security language when negotiating contracts where confidential data may be placed at risk.

Relatedly, FINRA stresses the importance of employee training, noting that many cybersecurity attacks resulted from ***employees "inadvertently downloading malware or responding to a phishing attack.***" FINRA found that 95% of the firms canvassed required mandatory cybersecurity training for staff.

Going forward, firms must balance the need to safeguard sensitive client information against the cost of adopting adequate cybersecurity measures. FINRA conveyed its expectation that broker-dealers consider the principles and best-practices set forth in the report when coordinating cybersecurity strategies, adding "FINRA will assess the adequacy of firms' cybersecurity programs in light of the risks they face."

National Law Review, Volume V, Number 40