The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 31539

January 2, 2019

FINRA Publishes Report on Selected Cybersecurity Practices

[31539]

January 2, 2019 TO: Chief Compliance Officer Committee
Internal Audit Committee
Small Funds Committee RE: FINRA Publishes Report on Selected Cybersecurity Practices

Earlier this month, the Financial Industry Regulatory Authority (FINRA) published a *Report on Selected Cybersecurity Practices – 2018*.[1] The report discusses FINRA's observations "regarding effective practices that firms have implemented to address selected cybersecurity risks while recognizing that there is no one-size-fits-all approach to cybersecurity."

The Report, which contains FINRA's observations regarding how broker-dealers are addressing cybersecurity concerns, is divided into five sections:

- Branch controls;
- Phishing;
- Insider threats;[2]
- Penetration testing;[3] and
- Mobile devices.

The discussion under each section concludes with FINRA summarizing effective practices its members have implemented to address concerns under each of these topics. The Report also includes an Appendix, "Core Cybersecurity Controls for Small Firms," that lists those core controls "that are likely to be relevant to many small firms' cybersecurity programs." The core controls listed and briefly discussed in the Appendix are:

- Patch Maintenance;
- Secure System Configuration;
- Identity and Access Management;
- Vulnerability Scanning;
- Endpoint Malware Protection;
- E-mail and Browser Protection;
- Perimeter Security;
- Security Awareness Training;
- Risk Assessments;
- Data Protection;

- Third-Party Risk Management;
- Branch Control; and
- Policies and Procedures.

Institute members interested in assessing the components and adequacy of their firm's cybersecurity program may find FINRA's observations to be meaningful. FINRA notes that the specific practices highlighted in the Report "should be evaluated in the context of a holistic firm-level cybersecurity program."

Tamara K. Salmon
Associate General Counsel

endnotes

[1] The 19-page report is available on FINRA's website at: http://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf.

[2] The discussion under Insider Threats is broken into the following subheadings, each of which includes FINRA's observations: Executive Leadership and Management Support; Identity Access Management and User Entitlements; Privileged User Controls; Security Information and Event Management and User and Entity Behavioral Analytic Tolls; Data Loss Prevention; Training; and Identifying Potentially Malicious Insiders.

[3] The Penetration Testing discussion has subsections relating to: Risk-Based Approach; Vendor Selection and Due Diligence; Contractual Arrangements; and Penetration Test Results.