News Release

For Release: Thursday, December 20, 2018
Contact(s): Ray Pellecchia (212) 858-4387

FINRA Publishes Report on Selected Cybersecurity Practices – 2018

WASHINGTON – FINRA today published its *Report on Selected Cybersecurity Practices - 2018*, a detailed review of effective information-security controls at securities firms. The report represents the newest initiative in FINRA's ongoing effort to help broker-dealers – including small firms – further develop their cybersecurity programs.

"Securities firms rate cybersecurity as one of their top operational risks, and our new report addresses areas that firms tend to find most challenging," said David M. Kelley, Surveillance Director, Member Supervision in FINRA's Kansas City office, referring to the report's five main topics:

- Cybersecurity controls in branch offices;
- Methods of limiting phishing attacks;
- Identifying and mitigating insider threats;
- Elements of a strong penetration-testing program; and
- Establishing and maintaining controls on mobile devices.

"Firms welcome the opportunity to see the effective practices used by other broker-dealers, so they can benchmark their controls and make informed decisions about establishing or evolving their own programs," said Yolanda Adewumi-Trottman, Examination Director, Member Supervision in FINRA's New York City office.

The new report builds on a 2015 cybersecurity report by FINRA that covered the main elements of a comprehensive cybersecurity program and provided guidance to firms seeking to improve their programs. The 2018 report adds greater depth and detail; for example, the section on branch controls lists more than three dozen specific, effective practices across written supervisory procedures, asset inventories, technical controls and branch review programs. The section on phishing highlights how to detect such attacks, including phishes that appear to be from trusted sources such as a CEO or other executive, the company help desk, customers or friends.

"There is no one-size-fits-all approach to cybersecurity, so FINRA has made a priority of providing firms with reports and other tools to help them determine the right set of practices for their individual business," said Steven Polansky, Senior Director, Member Supervision in FINRA's Washington, D.C. office. He recommended that small firms review the report appendix regarding core controls for such firms, as well as FINRA's previously published Small Firm Cybersecurity Checklist. All of these resources as well as a podcast and video based on the 2018 report are available at FINRA.org's cybersecurity topic page.

About FINRA

FINRA is a not-for-profit organization dedicated to investor protection and market integrity. It regulates one critical part of the securities industry – brokerage firms doing business with the public in the United States. FINRA, overseen by the SEC, writes rules, examines for and enforces compliance with FINRA rules and federal securities laws, registers broker-dealer personnel and offers them education and training, and informs the investing public. In addition, FINRA provides surveillance and other regulatory services for equities and options markets, as well as trade reporting and other industry utilities. FINRA also administers a dispute resolution forum for investors and brokerage firms and their registered employees. For more information, visit www.finra.org.