January 2019

FINRA report outlines cybersecurity practices

Key points

— FINRA has released a cybersecurity report to share “effective practices” to mitigate cyber risks in selected areas that FINRA says are most challenging to securities firms.
— The report is part of an ongoing FINRA initiative to help securities firms strengthen their cybersecurity programs.
— FINRA states that firms “routinely identify cybersecurity as one of their primary operational risks.”

FINRA released a Report on Selected Cybersecurity Practices that details information security controls FINRA has observed to be effective at securities firms in the areas of: branch controls, phishing attacks, insider threats, penetration testing, and mobile devices. The report follows FINRA’s 2015 report, which addressed the main elements of a firm-level cybersecurity program and provided guidance on program improvements.

FINRA notes that it continues to identify “problematic cybersecurity practices” through its examination and risk monitoring program and that firms “routinely identify cybersecurity as one of their primary operational risks.” FINRA states that the areas covered by the report are areas that firms tend to find the most challenging. A representative sample of the highlighted “effective practices” is provided below.

Branch office controls: FINRA states that a branch office’s autonomy from the home office can adversely affect a firm’s ability to implement a consistent firmwide cybersecurity program, especially in cases where a branch lags behind the head office in upgrading software and hardware or uses non-approved vendors. FINRA identifies the following “effective practices” for branch office controls:

— Establish written supervisory procedures to define minimum cybersecurity controls for branches and formalize oversight of branch office cybersecurity administration.
— Develop an inventory of branch-level data, software, and hardware assets.
— Identify and implement branch technical controls.
— Implement a branch cybersecurity examination and risk assessment program.

Phishing attacks: FINRA states that phishing attacks, where the sender of an email tries to convince a recipient to provide information or take action, are “one of the most common types of cybersecurity threats that firms discuss with FINRA.” Observed practices to mitigate the threat of phishing attacks include:

— Incorporating phishing scenarios in the firm-level risk assessment process.
— Establishing confirmation policies and procedures for transaction requests over a certain threshold.
— Regularly training employees on phishing and related firm policies and procedures.
— Regularly conducting simulated phishing email campaigns to evaluate employee understanding and compliance with policies and procedures.
— Imposing consequences for employees who repeatedly violate the firm’s phishing standards.

**Insider threats:** Insiders include individuals who currently have or previously had authorized access to firm systems and data and can include employees, contractors, and consultants. FINRA notes that effective insider threat programs typically integrate the following components:

— Executive leadership and management support, including the designation of a responsible senior manager.
— Identity and access management policies and technical controls, including heightened controls for individuals with privileged access and periodic reviews of user entitlements.
— Required training for all insiders.
— Measures to identify potentially abnormal user behavior in the firm’s network.

**Penetration testing:** Penetration testing, which simulates an attack on a firm’s computer network to determine vulnerability and evaluate protective measures, is a component in most firms’ cybersecurity program. FINRA notes that firms generally contract with third parties to perform penetration tests and also:

— Adopt a risk-based approach to penetration testing.
— Vet third-party testing providers.
— Establish contractual provisions that carefully prescribe vendor responsibilities.
— Rigorously manage and respond to penetration test results.
— Periodically rotate testing providers to benefit.

**Controls on mobile devices:** Mobile devices have emerged as a significant risk for many firms because of their increasingly widespread use by employees and customers. Firms with large numbers of retail customers may also be subject to greater exposure. Risks from mobile devices include malicious advertisements and spam communication; infected, cloned, or pirated mobile applications; vulnerabilities in mobile operating systems; and phishing, spoofing, or rerouting of calls, emails, and text messages. FINRA has observed “effective practices” to mitigate these risks, including:

— Prohibiting the use of personal devices for firm business unless approved.
— Providing regular training on mobile device requirements and effective security practices.
— Installing security software and antivirus software.
— Implementing reporting procedures for lost personal or firm devices.
— Ensuring the firm is able to remotely wipe firm data from a device that belongs to a former employee or from a lost device.
— Advising customers on the risks of making mobile devices “open” for unauthorized applications, games, and networking tools.
— Requiring multi-factor authentication for access to customer accounts and trading applications.

**Further steps**
FINRA notes that there is no "one-size-fits-all" approach to cybersecurity and recommends that the specific practices highlighted in this report should be evaluated in the context of a holistic firm-level cybersecurity program. Additional FINRA resources are available here.

**For additional information** please contact Charlie Jacco

---

**Contributing authors:**
Amy Matsuo, Principal and National Lead, Regulatory Insights
Karen Staines, Director, Financial Services Regulatory Insight Center
Phil MacFarlane, Associate Director, Financial Services Regulatory Insight Center

---

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. NDPSS 592774