Core Cybersecurity Controls for Small Firms

CONTACT US

Inquiries regarding this document may be directed to:

Steven Polansky
Senior Director, Member Supervision/Shared Services

(202) 728-8331

steven.polansky@finra.org

David Kelley
Surveillance Director, Member Supervision

(816) 802-4729

david.kelley@finra.org

The following list identifies core controls that are likely to be relevant to many small firms' cybersecurity programs. To establish an effective program, however, firms will need to consider these measures in the context of their business model and technology infrastructure, along with other factors that should inform firms' cybersecurity programs. In addition to this list of controls, FINRA has provided a number of cybersecurity resources for small firms. These include the 2015 FINRA *Report on Cybersecurity Practices* ("the 2015 Report"), the 2018 FINRA *Report on Selected Cybersecurity Practices* ("the 2018 Report") and FINRA's *Small Firm Cybersecurity Checklist* ("the Checklist"), as well as podcasts and webinars. Use of this list does not create a "safe harbor" with respect to FINRA rules, federal or state securities laws, or other applicable federal or state regulatory requirements.

- **Patch Maintenance.** Enable the automatic patching and updating features of operating systems and other software to help firms maintain the latest security controls (see Sections 4 and 5 of the Checklist).
- **Secure System Configuration.** When configuring systems and software, use vendor guidance or industry standards, such as those published by the Center for Internet Security ("CIS") (see Overview and Resources section of the Checklist).
- **Identity and Access Management.** Limit access to confidential customer and firm information based on business need. Tightly restrict use of "admin" or highly privileged entitlements and regularly review user accounts and privileges to modify or delete those which are no longer necessary to achieve business objectives (see the Insider Threats section of the 2018 Report, Technical Controls section of the 2015 Report and Section 8 of the Checklist).
- **Vulnerability Scanning.** Use Commercial Off-The-Shelf ("COTS") software or third-party vendors to continuously scan for vulnerabilities and quickly address detected discrepancies (see the Phishing section of the 2018 Report, the Cybersecurity Risk Assessment as well as Technical Controls sections of the 2015 Report and Section 10 of the Checklist).
- **Endpoint Malware Protection.** Install COTS software on firm computers, servers and firewalls to detect and block viruses and other malware (see the Technical Controls section of the 2015 Report and Sections 4 and 5 of the Checklist).

- **E-mail and Browser Protection.** Install software or use services to block web-based e-mail programs and unsafe content received through e-mail (*e.g.*, phishing attacks) or accessed via web browsers (see the Phishing section of the 2018 Report and Sections 4 and 5 of the Checklist).

- **Perimeter Security.** Use network access controls, such as firewalls, to block unnecessary connectivity between firm systems and outside systems. If feasible, incorporate an Intrusion Detection and Prevention capability (see the Insider Threats section of the 2018 Report, Technical Controls section of the 2015 Report and Sections 4, 5 and 10 of the Checklist).

- **Security Awareness Training.** Provide cybersecurity training to all employees upon their employment and at least annually thereafter (but preferably more often) to ensure all users are aware of their responsibilities for protecting the firm's systems and information. Training should address common attacks, how to avoid becoming a victim and what to do if you notice something suspicious. Consider implementing an ongoing phishing awareness campaign (see the Insider Threats section of the 2018 Report, Staff Training section of the 2015 Report and Section 8 of the Checklist).

- **Risk Assessments.** Conduct annual risk assessments and testing of firm controls to verify effectiveness and adequacy. This assessment may be accomplished using third-party or firm security experts (see Cybersecurity Risk Assessment section of the 2015 Report and Sections 1 and 2 of the Checklist).

- **Data Protection.** Encrypt critical data, back it up frequently and store copies of back-ups offline. Regularly test the firm's ability to restore data. Consider blocking USB ports and use of all removable data storage devices, including CDs and flash drives (see Sections 4, 5, 6 and 12 of the Checklist).

- **Third-Party Risk Management.** Review System and Organization Controls (SOC) or SSAE 18 reports for third party vendors and other partners with access to confidential firm and customer data to ensure they have security controls commensurate with, or better, than the firm's. All contracts should have provisions to enforce controls to protect data, including prompt notification of any changes to those controls and vulnerabilities or breaches that may affect the firm (see the Vendor Management section of the 2015 Report and Section 3 of the Checklist).

- **Branch Controls.** Ensure that branches apply and enforce relevant firm cybersecurity controls, which may include many of the controls identified in this list, as well as other relevant controls such as those elsewhere in this report or in the Small Firm Cybersecurity Checklist (see the Branch Controls section of the 2018 Report).

- **Policies and Procedures.** Create policies and procedures that address each category of controls applicable to the firm, such as those identified in this list (see the Governance and Risk Management for Cybersecurity section of the 2015 Report).

Investor protection. Market integrity.

1735 K Street, NW
Washington, DC 20006-1506

www.finra.org

18_0300.70 – 05/19