King & Spalding

Financial Services

Providing Strategic Legal Guidance to the Global Financial Services Industry

JANUARY 9, 2019

For more information, contact:

Russ Ryan
+1 202 626 5457
rryan@kslaw.com

Mirella deRose
+1 212 827 4083
mderose@kslaw.com

Russell Johnston
+1 212 827 4081
rjohnston@kslaw.com

Richard Margolies
+1 212 827 4080
rmargolies@kslaw.com

Carmen Lawrence
+1 212 556 2193
clawrence@kslaw.com

Michael Watling
+1 212 827 4082
mwatling@kslaw.com

King & Spalding

New York
1185 Avenue of the Americas
New York, New York 10036-4003
Tel: +1 212 556 2100

FINRA Offers Member Firms Continued Guidance on Cybersecurity

On December 20, 2018, the Financial Industry Regulatory Authority (FINRA) issued a "Report on Selected Cybersecurity Practices" (the "Report") as part of its ongoing efforts to assist broker-dealer firms in developing effective cybersecurity programs.[1] This new Report builds upon FINRA's 2015 Report on Cybersecurity Practices and its publication in May 2016 of a recommended Small Firm Cybersecurity Checklist. It also echoes many of the "highlighted observations" that were prominently featured in FINRA's 2017 Report on Examination Findings.[2]

The Report highlights FINRA's observations regarding effective cybersecurity practices in the following five key areas:

BRANCH LOCATION CONTROLS

Noting that remote branch offices present particular cybersecurity challenges, the Report provides granular examples of effective practices FINRA has observed in each of these four primary areas:

- Developing and distributing branch-level written supervisory procedures and guidance on cybersecurity controls, including designating the branch office supervisor with responsibility for cybersecurity oversight;
- Developing and utilizing an inventory of branch-level data, software, and hardware assets;
- Implementing technical controls to mitigate the most significant threats to branch-level data and systems; and
- Implementing a robust branch cybersecurity examination program.

DEFENDING AGAINST "PHISHING" ATTACKS

Recognizing that phishing attacks are among the most common cybersecurity threats firms have discussed with FINRA, the Report offers a dozen examples of effective practices it has observed across the industry. The list includes creating policies and procedures to directly address

phishing, technical defenses, training and risk-assessment scenarios, documentation of phishing attempts, and reporting to government authorities and information-sharing organizations.

INSIDER THREATS

The Report identifies insider threats as a key cybersecurity risk for many firms – specifically employees, contractors, and vendors with current or past access to firm systems and data who may be motivated to disclose or misuse this information. FINRA offers detailed observations of effective practices in seven areas relevant to mitigating insider threats:

- Support and commitment from executive leadership and management with respect to cybersecurity;
- Establishing effective identity-access-management ("IAM") and user-entitlement processes;
- Establishing strict controls for "privileged users" with access to powerful system commands and utilities, so that they have access to only those privileges necessary for their job function and do not abuse their privileges;
- Making effective use of Security Information and Event Management ("SIEM") and User and Entity Behavioral Analytic ("UEBA") tools;
- Establishing and implementing a strong Data Loss Prevention ("DLP") program and related controls;
- Adopting an effective, ongoing training program for employees, contractors, and vendors; and
- Using people, processes, and technology to identify potentially ill-motivated insiders.

PENETRATION TESTING

The Report notes that many firms have effectively used penetration testing – a test designed to simulate an attack on a firm network to determine the degree to which malicious actors may be able to exploit vulnerabilities – in their ongoing efforts to defend against cybersecurity threats. It lists five specific observations of effective practices in this area:

- Adopting a risk-based approach to penetration testing;
- Thoroughly vetting testing providers;
- Using contractual provisions that carefully prescribe vendor responsibilities;
- Rigorously managing and responding to penetration test results; and
- Periodically rotating testing providers.

MOBILE DEVICES

The Report observes that as firm employees, customers, consultants, and contractors have become more reliant on mobile devices to conduct firm business, risks associated with the technology have likewise increased, particularly for firms with large numbers of retail customers. FINRA provides a useful list of more than two dozen specific practices that firms have adopted to combat potential attacks on sensitive customer and firm information, including:

- Developing specific mobile devices policies and procedures;
- Placing appropriate restriction on use of personal devices;
- Providing regular training to employees, consultants, and contractors;
- Maintaining an inventory of all devices;

- Requiring encryption along with adequate password length and complexity;
- Installing effective security and antivirus software;
- Educating customers about the security risks associated with using mobile devices to communicate with the firm;
- Using multi-factor authentication for customer account access; and
- Timing-out of access to systems after a certain period of inactivity.

FINRA's Report explicitly cautions that it does not create or change any existing regulatory requirements, and that adopting the recommended practices and procedures in the Report will not create a "safe harbor" from liability. Nevertheless, the Report provides useful benchmarking information and an excellent starting point for firms struggling to keep up with evolving cybersecurity risks.

[1] *FINRA Report on Selected Cybersecurity Practices – 2018*, available at www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf.
[2] *Report on FINRA Examination Findings* (December 2017), available at www.finra.org/sites/default/files/2017-Report-FINRA-Examination-Findings.pdf. Cybersecurity was not among the featured observations in FINRA's most recent examination findings report issued in December 2018.