CARLTON FIELDS

FINRA's New Report on Broker-Dealer Cybersecurity Practices

March 06, 2019

The protection of customer personal data continues to be a priority for the Financial Industry Regulatory Authority (FINRA), primarily from an examination perspective and, the author predicts, increasingly from an enforcement perspective. In its December *Report on Selected Cybersecurity Practices—2018*, FINRA shares information learned during its examinations to help broker-dealer firms to increase the effectiveness of their cybersecurity programs. Attention to this report will assist even the most sophisticated firms in both strengthening their data security controls and responding to FINRA examination requests.

This articles first summarizes the key regulations that govern broker-dealers' data management and protection efforts. The article then describes the key points of the report. Finally, it offers some observations from the author's practice, to amplify the suggestions in FINRA's report.

The Legal Landscape for Protection of Customer Data

With respect to member cybersecurity practices, FINRA has focused its efforts on ensuring compliance with Security and Exchange Commission (SEC) regulations on privacy and data integrity and security. The main three of those regulations, as listed by FINRA in its public statements on cybersecurity, are described below.

First, Regulation S-P (17 C.F.R. § 248.30) requires, among other things, that firms adopt written policies and procedures to secure the confidentiality of customer records and information, and to protect those records against anticipated threats and unauthorized access. Regulation S-P also demands immediate and annual disclosure to customers of a firm's privacy policies and practices. In addition, the regulation governs the disclosure of nonpublic personal information and account number information that is permitted to unaffiliated third parties.

Second, Regulation S-ID (17 C.F.R. § 248.201–202) requires that securities firms implement a written program to detect, prevent, and mitigate identity theft in connection with certain customer accounts. Those accounts include retail brokerage accounts or any other personal accounts with a reasonably foreseeable risk to customers from identity theft.

Third, the Securities Exchange Act of 1934 (17 C.F.R. § 240.17a-4(f)) requires that firms that keep records by means of "electronic storage media" maintain those records in a "non-rewriteable, non-erasable format" and in such a way that it will "verify automatically the quality and accuracy of the storage media recording process." The requirement to preserve electronic records in this way, sometimes known as the "write once, read many" (or "WORM") format, was the basis for the $14.4 million in fines against 12 firms that FINRA announced in December 2016.

Of these regulations, perhaps Regulation S-P is the most important to examinations, as it is broadest in scope and can often be made to fit, fairly or unfairly, a wide range of a firm's data protection conduct.

FINRA's *Report on Selected Cybersecurity Practices—2018*

FINRA's review of cybersecurity programs under these regulations is, perhaps surprisingly, technical in nature. That is, it includes not just an assessment of systems governance, policies and procedures, and staff training, but also a review of risk assessments, technical controls, and system change management. Examinations may also test incident response planning, vendor management, and active data loss prevention.

Member firms facing these inquiries will find that responding to some are straightforward, such as proving both staff trainings and risk assessments, because those tasks can be largely outsourced to third parties along with the proof of same. But other areas of cybersecurity readiness must be integrated into business practices on a continual basis, including general technology governance and incident response preparedness. Those are also harder for a firm to track over time and for FINRA to measure and benchmark.

It is into this regime that FINRA's new report, released on December 20, 2018, enters. It is the first such report in three years, and it goes into considerable detail on what FINRA has learned from its examination program. A practitioner in this area should study it in its entirety, but a few highlights follow.

First, the report observes that "some firms face challenges maintaining effective cybersecurity controls at their branch locations." FINRA notes that branches tend to have less developed

cybersecurity controls than the home office and that an effective practice would include developing "branch level" written supervisory procedures (WSPs) addressing "comprehensive guidance." The report also suggests that an "asset inventory" be completed at the branch level so that the firms know "the scope of assets they need to protect." Finally, FINRA names as an effective practice that the home office conduct "periodic exam visits or risk-based audits" at each of the branches.

Second, the report discusses "phishing"—the use of deceptive emails or other e-messages to spread malware or fraudulently obtain information or money—as "one of the most common cybersecurity threats firms have discussed with FINRA." Consistent with common guidance for controls against social engineering cyber attacks, FINRA names the following, among others, as effective practices: training, email scanning and filtering, simulated attacks, segmenting customer assets and information, and multifactor authorization.

Third, the report details the causes of, and possible prevention and mitigation of, insider threats, which are threats to data security from those who already have access to firm systems and can therefore circumvent many firm controls designed only to repel third-party access. FINRA recommends ensuring "proper access" to data, including "that systems entitlements are aligned with specific job functions and assigned only on a need-to-know basis." This is sometimes known as the "policy of least privilege," and in its simplest form, it ensures that a summer intern, for example, is not provided a username and password that would allow unlogged access to account data for the firm's entire customer and lead database.

Fourth and finally, the report describes the risk and potential controls over threats to data integrity from the proliferation of mobile devices. FINRA notes as effective practices robust "bring your own device" standards, removal of applications that violate the firm's policies, and reporting procedures for lost or stolen devices, including personal devices with access to firm data.

Additional Considerations for the Industry

In light of FINRA's conclusions in its report, and in consideration of the author's observations from practice, there are four additional points to consider. Because the report focuses in large part on prevention rather than on mitigation during a breach, the first two suggestions that follow attempt to highlight the critical role that breach response can have in limiting the scope of a data loss incident.

First, each firm should review, test, and, if necessary, revise its incident response plan. This plan is in addition to the WSPs, which should set out the cybersecurity controls themselves. The incident response plan should focus instead on what to do in the event of an actual or suspected breach of customer personal information. The incident response plan should be a user-friendly document that sets out a process for how data security incidents are identified, reported, escalated, mitigated, and remediated.

To this end, most incident response plans benefit from having at least the following two attachments. The first is the internal list of contacts to join the incident response team in the event of a data security incident, with after-hours contact information and secondary contacts for each position. The plan itself would offer guidance by role and responsibility, but this attachment should have the actual names and mobile numbers of the primary and secondary employees. The second attachment should include the preapproved vendors to assist in the event of a data breach, including insurance broker, cybersecurity expert, legal assistance, and media relations team. An additional best practice: The key contact could call those individuals periodically to check in and remind them that they may receive an emergency call.

As a second key point, each firm should name a single point of contact for interaction with the regulators in the event of a data incident, and train that individual as part of the incident response planning. The report suggests in a few places that a firm designate an individual officer (or branch manager) as being ultimately responsible for cybersecurity, which is sound advice. But this suggestion is for a different role. Rather than being the person responsible for the cybersecurity *controls*, this person is ultimately responsible for *reporting* an incident to FINRA or other third parties, which often requires a different, nontechnical skill. This professional need not be—and often should not be—a cybersecurity expert, because during an incident, the technical cyber expert will be working on investigating and remediating the incident. The suggested role may be better suited for the employee who has regular interaction with the firm's FINRA regulatory coordinator. This person should also receive training on, and perhaps meet in advance with, the local Federal Bureau of Investigation field office, which is typically the point of contact for larger-scale data security incidents affecting the securities industry or markets.

As a third key point from the report, certain firms have a profile that makes an incident more likely or, if it occurs, more damaging to the customers and the firms. The report noted the risks from branch offices. Three additional profiles include those firms experiencing rapid growth, those serving aged investors, and those undergoing a merger with other firms. Rapid-growth firms are often adding customers and opportunities faster than their technical systems can grow to match. Elder investors present particular challenges for data security, including an increased risk of being a victim of identity theft, Internet-related scams, and other forms of elder abuse that manifests as a threat to data integrity. Finally, firms that are merging or acquiring or being acquired may see technical challenges to protection (or risk inadvertent disclosure) in the integration of systems. Firms with these profiles need to be particularly attendant to cyber risk.

As a fourth key observation, mentioned in a few areas in the report, firms should focus resources on vendor management for cybersecurity. This is when a firm studies the data security controls of those with whom it contracts or subcontracts to process, collect, or hold customer data or those third parties that, through contract relationships with the firm, have access in some capacity to its systems. This inquiry would include ensuring not only that vendors trusted with the firm's customer

data have sufficient technical controls but also that vendors—including those that do not possess the firm's customer data—cannot be used as a bridge to access data on the firm's servers. Such a focus would include reviewing vendor contracts to determine whether vendors have agreed to appropriate data management practices, to specify how notice will be made to firm customers in the event of an incident at the vendor affecting customer data, and to shift liability as appropriate between the firm and the vendor. A firm with several vendors, each of which holds its customers' personal information or has system access in whole or in part, will typically benefit from a review of the overall relationship structure and possible consolidation.

Conclusion

The new FINRA *Report on Selected Cybersecurity Practices* provides granular, technical advice to broker-dealers on developing and strengthening cybersecurity protections for customers. While FINRA was not explicit that this list of "effective practices" would be the basis for potential investigations and enforcement actions in the future, it is a fair inference from the report's detail that these examples and trends are more than just general nudges toward better practices. Indeed, FINRA's 2019 Risk Monitoring and Examination Priorities Letter indicates that the report's suggestions may form the basis, in whole or in part, for future, more detailed regulation of industry participants.

Republished with permission from the American Bar Association, this article was drafted in conjunction with an ABA regional CLE workshop, "Second Annual Current Issues in FINRA Arbitration and Enforcement," held February 22, 2019, in Tampa, Florida. The workshop was cosponsored by the Securities Litigation Committee and the Privacy & Data Security Committee of the Section of Litigation.

Authored By

John E. Clabby

Related Practices

Cybersecurity and Privacy
Litigation and Trials
FINRA Enforcement, Arbitration, and Appeals