Client Alert

February 25, 2015

FINRA Issues its Cybersecurity Report, Providing Tools and Encouragement to Broker-Dealers

By Daniel A. Nathan

FINRA recently issued a Report on Cybersecurity Practices ("Report"), growing out of its targeted examination of firms last year. To issue the Report, FINRA gave careful consideration to the needs of many broker-dealers for information and the tools to combat cyber intrusions. The Report is comprehensive, and it doesn't shy away from delving into technical detail. Our review of it leads us to conclude that it is a useful resource for broker-dealers looking to assess and improve their procedures for preventing a cybersecurity attack, and dealing with one if and when it comes.

At the same time, FINRA also issued guidance to enable investors to understand the state of their firms' data protection by issuing a new Investor Alert entitled "Cybersecurity and Your Brokerage Firm." The Alert recommends that investors ask their firms about: the safeguards they have in place to protect personal information and assets; the procedures the firm uses to monitor investors' personal information; the firms' approaches to handling cyber events; whether the firms will reimburse investors if their assets are compromised due to a cyber attack; and what measures the firms recommend investors take to personally protect their information.

FINRA's Report (together with the SEC's recent cybersecurity report) should provide the motivation and some of the tools needed by those broker-dealers who have put off focusing on this area to roll up their sleeves, and additional motivation will come from the firms' own customers.

This Client Alert cannot hope to summarize the 45-page Report, and we encourage those firms embarking on a cybersecurity project to read the entire Report. Here we will point out some of the most relevant observations and recommendations in the Report, with a view to encouraging broker-dealers to review their procedures and adopt the recommendations as appropriate.

GENERAL PRINCIPLES

As FINRA's Report indicates, cybersecurity has been a regular theme in its annual Regulatory and Examination Priorities Letter since 2007, and over the years FINRA has conducted surveys and on-site reviews of firms to increase its awareness of how firms control cyber risks. FINRA points to a variety of factors driving firms' exposure to cybersecurity threats, including advances in technology, changes in firms' business models, and changes in how firms use technology. A prime example of such risks is the increased use of web-based access or mobile devices for brokerage activities.

FINRA defines "cybersecurity" as "the protection of investor and firm information from compromise through the use . . . of electronic digital media." "Compromise" is the loss of data confidentiality, integrity or availability.

FINRA acknowledges that there is no "one size fits all" approach, because firms come in a variety of sizes and business models, and acceptable approaches to compliance and supervision may vary widely among firms. But at the end of the day, "firms must have appropriate risk management measures in place to address the cybersecurity-related threats they face."

FINRA's Report is perhaps at its most useful when it reviews practices that it observed at firms in each area discussed; these discussions will permit broker-dealers to benchmark their practices against the industry in general, and increase the urgency of improving their systems when they find that they fall short.

GOVERNANCE AND RISK MANAGEMENT

A defined governance framework will enable a firm to make decisions about establishing policies and procedures, selecting, implementing and monitoring controls, and establishing an independent assessment function. The governance framework should describe the leadership role that the board of directors (if the firm has one) should play in overseeing the firm's cybersecurity, and that role will require the board, among other things: to understand that cybersecurity is an enterprise-wide risk management issue; to have access to expertise in the area; and to set expectations for management to establish a risk management framework with adequate resources.

The Report notes the benefits to greater board involvement in ensuring that firms adequately focus on cybersecurity. As evidence, the Report cites to FINRA enforcement actions related to cybersecurity that frequently made findings of significant governance or management failures – for example, failures to act on warnings that, if heeded, could have mitigated the loss of customer information. In the Report, FINRA identifies existing industry frameworks and standards that firms can draw upon in developing their approach to cybersecurity, including those created by the National Institute of Standards and Technology, the International Organization for Standardization and International Electrotechnical Commission, and the ISACA, which FINRA found are used by almost 90 percent of the firms reviewed.

CYBERSECURITY RISK ASSESSMENT

FINRA recommends that firms conduct regular assessments to identify cybersecurity risks, and give priority to remediating these risks. FINRA explains that these risk assessments should focus on specific broker-dealer-oriented risks, that is, the compromise of customer or firm confidential information, misuse of customer assets, and theft of proprietary trading algorithms. And, of course, FINRA points out the risk of harm to a firm's reputation in the event of a breach.

A risk assessment should ensure that a firm's controls are adequate to prevent harm, detect potential threats, correct a system after a detrimental event, and predict the possibility of an event occurring. The Report lists fifteen areas in which a firm might want to improve its controls, including controls governing data storage at vendors, employee access, or Wi-Fi protection.

INCIDENT RESPONSE PLANNING

The general assumption for designing cybersecurity procedures and controls is that it is not a matter of *if* a cyber event might occur, but *when*. Firms must have an incident response plan that will prepare them to manage a cybersecurity event in order to limit damage, maintain the confidence of external stakeholders, and reduce

recovery time and costs. FINRA points to firms that have a dedicated Computer Security Incident Response Team, and for smaller firms approves the step of contracting with a knowledgeable vendor to provide incident response capability.

FINRA cites these incident response steps:

- Containment to prevent an incident from further damaging a firm, and mitigation of any damage;
- Eradication of any causes of the incident, and recovery of systems to restore them to normal operation;
- Investigation of the incident to determine the extent of loss and identify the causes;
- Notification of all relevant parties, including regulators and, where appropriate, customers; and
- Making clients whole, including providing free credit monitoring services and reimbursing customers for losses.

VENDOR MANAGEMENT

Even if a firm has established state-of-the-art internal controls and procedures, it remains vulnerable if it does not ensure that the third-party vendors that it uses – for example, for cloud-based services – are not themselves a source of cybersecurity risks. A vendor or its employees could misuse firm data, or the vendor itself could be subject to cyber attack.

The Report provides an extensive list of suggestions for controlling this potential risk area. The recommended practices include:

- Initial due diligence on prospective vendors;
- Contractual provisions that set out the vendor's obligations for protecting firm information and permit ongoing oversight of the vendor, among other things; and
- Ongoing due diligence of a vendor's controls and processes.

STAFF TRAINING

Even with adequate systems and controls, a firm's employees who do not adequately understand and apply them can be weak links and high risk areas. Cybersecurity training therefore is an essential component of any program, and the Report provides suggestions for the content and frequency of such training. The good news is that 95 percent of firms reviewed already provide mandatory cybersecurity training for their staff; the bad news is that those firms that do not will probably be easily identifiable as outliers.

OTHER AREAS

Technical Controls: The Report reviews technical controls approaches in general and specific types of controls to protect firm software and hardware as well as firm data. The discussion is highly technical and will be of value to the IT departments or vendors who are assigned those responsibilities.

Cyber Intelligence and Information Sharing: Firms need to keep up with intelligence about cyber threats – through assigned staff or outside vendors – in order to maintain protections against any new or emerging threats. In addition, firms should participate in information-sharing protocols to benefit from available information about new technologies and recent attacks.

Cyber Insurance: The market for cyber insurance is evolving rapidly, and in some cases costs are decreasing as the number of participants increase and the need for coverage becomes more apparent. There are a variety of cyber insurance plans that provide a range of types of coverage. The Report points out that the evolving nature of cyber threats compels many firms to review their coverage annually.

RECOMMENDATION

Without taking a position on which controls and procedures discussed in FINRA's lengthy Report are more important or effective, it is easy for us to simply recommend that key personnel at all broker-dealers read the Report. After reading it, officials at many firms will derive satisfaction from knowing that they are up-to-date with all of its recommendations and, indeed, that they themselves were the subjects of the best practices that FINRA reports to the industry. Many firms will find that they are largely on point, but will identify some gaps that are worth filling in the interest of having a more effective system. And some firms will have been waiting for this "wake up call" to start the necessary process of putting a system in place. With the benefit of these and other resources, they might find that the job is not as daunting as they feared.

Contact:

Daniel A. Nathan
(202) 887-1687
dnathan@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.