Bloomberg BNA

Privacy and Security Law Report®

Going for Brokerages: FINRA and SEC Take Aim at Deficient Cyber Policies and Practices

By Mark Mermelstein, Aravind Swaminathan, Daniel J. Dunne and Antony P. Kim

On Feb. 3, the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) each released reports regarding cybersecurity issues for brokerage and advisory firms, both of which **should be considered required reading for chief information security officers, chief information officers, legal teams and anyone else responsible for managing cybersecurity risk.**[1] These reports highlight best practices for managing cybersecurity risk and areas for potential improvement, and should encourage firms to consider further investments in cybersecurity because, as FINRA specifically points out, it ''expects firms to consider the principles and effective practices presented in the report as they develop or enhance their cybersecurity programs.''[2] As a result, firms should anticipate that elements covered in the reports will be benchmarks for measuring the effectiveness of a firm's cybersecurity program in any enforcement action brought by either the SEC or FINRA.

The SEC's National Exam Program Risk Alert, ''Cybersecurity Examination Sweep Summary,'' summarizes the cybersecurity policies and practices of 57 registered broker-dealers and 49 registered investment advisers based on examinations conducted by the SEC's Office of Compliance Inspections and Examinations (OCIE). FINRA's more detailed ''Report on Cybersecurity Practices'' also summarizes cybersecurity programs at a broad array of firms, but it goes further, making the FINRA report particularly important for a number of other reasons. First, the report makes clear that FINRA has been active in bringing cybersecurity-related enforcement actions against both firms and individual executive officers when customer data are put at risk or compromised. Careful review of these case studies highlights factors that FINRA considers important in determining whether firms have satisfied their cybersecurity obligations. Second, the report sets out a series of detailed principles and effective practices for risk assessments, incident response plans and governance, among others. These principles and practices offer a road map for cybersecurity planning and risk management and establish baseline standards to which FINRA will hold firms accountable. Finally, the report provides very specific recommendations that firms can operationalize, demonstrating FINRA's sophistication in cyber and data security matters.

SEC and FINRA Reports Conclude Extensive Investigations

On March 26, 2014, the SEC sponsored a Cybersecurity Roundtable, highlighting the role of cybersecurity in ensuring the integrity of the market system (13 PVLR 550, 3/31/14). On April 15, 2014, the OCIE announced that it would conduct a series of examinations to ''assess cybersecurity preparedness in the securities indus-

[1] SEC, National Exam Program Alert, Vol. IV, Issue 4, ''Cybersecurity Examination Sweep Summary'' (Feb. 3, 2015), *available at* http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf; FINRA, *Report on Cybersecurity Practices* (Feb. 2015), *available at* http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf (14 PVLR 242, 2/9/15).

[2] FINRA, *supra* note 1, at 2.

try and to obtain information about the industry's recent experiences with certain types of cyber threats.''[3] As part of its examination, the OCIE explained that it would focus on: cybersecurity governance; identification and assessment of cybersecurity risks; protection of networks and information; risks associated with remote customer access and fund transfer requests; risks associated with vendors and third parties; detection of unauthorized activity; and experiences with certain cybersecurity threats. Although the OCIE spent considerable time gathering information relating to practices and policies, it did not conduct any technical review of firms' cybersecurity programs.

Similarly, in early 2014, FINRA initiated a yearlong examination of cybersecurity programs across a broad cross-section of regulated firms, including large investment banks, clearing firms, online brokerages, high-frequency traders and independent dealers. FINRA's objectives were to better understand the threat landscape, risk exposure and management strategies, and to share these findings with firms in order to provide them with a road map for developing an effective cybersecurity program. The report builds on FINRA's 2011 survey of 224 firms, with interviews of other organizations involved in cybersecurity, previous FINRA work on cybersecurity and publicly available information. Although it is not meant to cover all areas of cybersecurity, the report focuses on the key elements of an effective, risk management-driven cybersecurity program: governance and risk management; risk assessments; technical controls; incident response planning; vendor management; staff training; cyber intelligence and information sharing; and cyber insurance.

FINRA 'Case Studies' Provide Valuable Enforcement Insight

Both the SEC and FINRA reports are based, in large part, on extensive surveys conducted at broker-dealer firms and advisers. The SEC notes that the vast majority of broker-dealers (88 percent) and advisers (74 percent) said they had experienced a cyberattack of one kind or another. The SEC offers an important perspective on what organizations with mature and effective cybersecurity programs are doing and where the industry has room for improvement. For example, the most common attacks continue to be simple fraudulent e-mail scams, which were successful more than 25 percent of the time. And although broker-dealers generally reported these events to the Financial Crimes Enforcement Network (FinCEN), very few reported these cases to law enforcement.

FINRA's report makes clear that it actively monitors firms' cybersecurity programs—especially in the wake of a data breach—while recognizing that cybersecurity programs are not a one-size-fits-all proposition. Each firm must craft a program that is tailored to specific technical and policy considerations.

For example, the FINRA report outlines an enforcement action against a firm that suffered a compromise resulting in the theft of approximately 200,000 customer profiles (names, account numbers, Social Security numbers, dates of birth, etc.). Even though the firm had conducted penetration testing of its systems, it failed to include in the scope of the test a database of unencrypted customer data. FINRA found that, had the firm properly inventoried databases with sensitive information or better scoped its penetration testing, it could have detected critical weaknesses in password management and holes in encryption procedures that would have aided in preventing the incident. FINRA went forward with an enforcement action, fining the firm $375,000 for alleged violations of Rule 30 of Regulation S-P, National Association of Securities Dealers (NASD) Rule 2110 and NASD Rules 3010(a) and (b).[4]

The FINRA report also highlights another tool in its cybersecurity toolbox through case studies of two enforcement actions. In both cases, online firms opened a number of accounts in the ordinary course of business for high-risk foreign customers. After successfully opening the online accounts, these customers hacked into accounts held at other online broker-dealers and engaged in fraudulent short-sale and ''pump and dump'' trading transactions through the firms' Direct Market Access platform. In each instance, the firms failed to implement a reasonably designed customer identification program as part of their anti-money laundering (AML) procedures. This failure could have been remedied had the firms used better identity and access management (IAM) policies. FINRA brought enforcement actions against each of the firms, alleging violations of NASD Rules 3110(a) and (b) and NASD Rule 2110. Both firms settled, with one agreeing to pay a $300,000 fine and hire (at its own expense) a monitor to review compliance with the firm's AML procedures.[5]

Other cyber-related factors that FINRA considered in enforcement actions include:

- failure to timely remediate a device that was exposing customer information to unauthorized users;
- failure to conduct an adequate breach incident response investigation;
- failure to act on warnings that could have substantially mitigated the loss of customer information;
- inadequate user access restrictions;
- inadequate vendor oversight or supervision of outsourcing arrangements;
- failure to conduct adequate, periodic cybersecurity assessments;
- failure to review, or to establish procedures for reviewing, Web server logs that would have revealed data theft/loss;

[3] SEC, National Exam Program Alert, Vol. IV, Issue 2, *OCIE Cybersecurity Initiative* (Apr. 15, 2014), *available at* http://www.sec.gov/ocie/announcement/Cybersecurity%20Risk%20Alert%20%20%2526%20Appendix%20-%204.15.14.pdf (13 PVLR 673, 4/21/14).

[4] D.A. Davidson & Co., FINRA Letter of Acceptance, Waiver and Consent, No. 20080152998 (Apr. 9, 2010), *available at* http://disciplinaryactions.finra.org/Search/ViewDocument/37555 (9 PVLR 550, 4/19/10).

[5] Pinnacle Capital Markets, LLC FINRA Letter of Acceptance, Waiver and Consent, No. 2006006637101 (Dec. 17, 2009), *available at* http://disciplinaryactions.finra.org/Search/ViewDocument/15323 (9 PVLR 229, 2/8/10); Manhattan Beach Trading Financial Services, Inc., FINRA Letter of Acceptance, Waiver and Consent, No. 2010023995101 (May 30, 2012), *available at* http://disciplinaryactions.finra.org/Search/ViewDocument/31845.

- failure to have written policies and procedures in an information security program designed to protect confidential customer information;
- failure to heed a prior auditor recommendation to acquire an intrusion detection system; and
- weak IAM policies.

Even in the aggregate, these are easily remedied shortcomings that could have been avoided through proactive cybersecurity assessments, governance and mitigation strategies. And, as the report makes clear, they will be areas of focus in any cybersecurity-related enforcement investigation or proceeding.

Principles and Effective Practices

While the enforcement actions illustrate ''floor'' considerations for any cybersecurity program, the SEC and FINRA reports also offer specific, granular guidance on best practices and considerations that firms should consider implementing or adopting across eight significant areas of cybersecurity:

1. *Governance and Risk Management*: FINRA's report devotes a considerable portion of its discussion to implementing cybersecurity governance and risk management mechanisms. Specifically, it recommends clearly defining a governance framework that supports intelligent, fact-based decision-making by senior managers (and where relevant, board-level officers) that is based on risk appetite and assessment. The absence of strong cybersecurity governance significantly increases regulatory risk under Rule 30 of SEC Regulation S-P or SEC Regulation S-ID. Accordingly, senior management and board involvement in enterprisewide cybersecurity risk management are critical to establishing priorities and responding to cybersecurity threats, especially because they facilitate adequate resources allocation necessary to address cybersecurity risks. Moreover, because of the importance in performance measurement (and communication and expertise gaps that lie between cybersecurity professionals and executives), both the SEC and FINRA place significant emphasis on using external standards and frameworks, such as the National Institute of Standards and Technology ''Framework for Improving Critical Infrastructure Cybersecurity'' (Version 1.0),[6] as key management tools to assess cybersecurity posture and risk effectively. While executives and directors may not be able to appreciate the technical aspects of a cybersecurity program, they are accustomed to using relative relationship assessments to make informed decisions about risk. Accordingly, limited reliance upon metrics or outright failure to use them in the foregoing manner will likely be a factor in making enforcement decisions.

2. *Cybersecurity Risk Assessment*: The key to any cybersecurity assessment is the effective identification and inventory of data assets (a particularly important consideration for broker-dealers under Regulation S-P) and physical assets (e.g., endpoints, mobile devices) with access to the firm's network. Using an accurate asset inventory, firms can focus assessments of external and internal threats and vulnerabilities and prioritize remediation efforts accordingly. FINRA notes its concern that approximately 20 percent of firms surveyed either had no assessment program or one that was in its nascent stages. FINRA cautions that the remaining 80 percent should not get complacent, and it recommended regular assessments that are indexed to the changing threat landscape. Moreover, these assessments should not only target high priority assets but should also draw from a broad array of inputs (historic, current, industry trends) to be correctly and adequately scoped.

3. *Technical Controls*: FINRA recommends implementing a defense-in-depth strategy that relies both on the overall network architecture and individual controls, with an emphasis on IAM polices, data encryption and penetration testing. As FINRA points out, IAM presents one of the most critical challenges because weak access management can be exploited by both inside and outside attackers and undermine AML controls. Accordingly, FINRA expects firms to establish policies and procedures that rely on the policy of least privilege (PoLP), separation of duties (SoD) and entitlement transparency principles, combined with use monitoring, access reviews, provisioning and prompt access termination. Recognizing that encryption plays a key role in defending data, FINRA recommends a more sophisticated approach that involves implementing encryption for both data at rest and data in transit at multiple levels in connection with a defense-in-depth strategy. Finally, FINRA recommends penetration testing that is calibrated to asset inventories and cybersecurity priorities established in the governance phase.

4. *Incident Response Planning*: FINRA recommends that firms develop comprehensive, but flexible, incident response plans. These plans should include preparation, incorporation of current threat intelligence, containment and mitigation strategies, investigation and assessments, eradication and recovery and post-event communications and notification strategies, the last of which may be governed not only by state laws but also by Regulation S-ID and FINRA Rule 4530(b). FINRA strongly cautioned that simply deploying a general ''check-the-box'' plan is not enough. Firms should craft incident response plans for a variety of attack scenarios that align with threat landscape assessments and tabletop such plans to identify areas for improvement and training opportunities. As part of such incident response planning, and to maintain customer confidence and address investor losses, FINRA encourages firms to provide free credit monitoring services and reimburse clients who have suffered losses as the result of a cyberattack.

5. *Vendor Management*: With the rise in cybersecurity incidents traced to vulnerabilities in vendor systems and access, both FINRA and the SEC note the importance of conducting cybersecurity assessments and due diligence of vendors, both at the inception and throughout the engagement. Too few firms, according to the SEC, subjected their vendors to the same quality of testing and assessment as they did for their own systems, or required those vendors to conduct self-assessments by incorporating security requirements into vendor agreements. FINRA recommends a variety of diligence tools such as survey questionnaires, ongoing review of third-party control assessment reports and on-site verification audits and reviews, depending on the access to data and networks and the risk profile of the firm. Similarly, required controls should be indexed to the associ-

[6] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (13 PVLR 281, 2/17/14).

ated risk level and potentially include the following: limits on vendor data access, encryption, patch management and anti-virus/malware protections, subcontractor controls, ethical hacking of online systems and recovery processes. Both the SEC and FINRA emphasize incorporating security requirements directly into vendor agreements, with FINRA encouraging firms to prepare contractual template provisions in advance to facilitate the use of vendor management in the following areas: nondisclosure; data storage, retention and delivery; breach notification responsibilities; security audits; employee access limitations; and use of subcontractors.

6. Staff Training: Recognizing that employees are one of the largest cybersecurity risks, FINRA recommends tailored trainings that include interactive training developed, regularly refreshed and deployed in the context of threat intelligence, prior security incidents and risk assessments. Firms with exceptional cybersecurity programs have even developed modules for customer education and training, recognizing that cybersecurity threats may originate from clients. Simulations can be a particularly valuable training opportunity because they allow firms to develop a better understanding of potential policy weaknesses and human vulnerabilities that can be used to develop further tailored training.

7. Cyber Intelligence and Information Sharing: The SEC notes that better-prepared firms made more extensive use of industry information-sharing networks, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) or the National Cyber Forensics and Training Center, peers and conferences to identify best practices to improve their own cybersecurity programs. Similarly, FINRA recommends that firms designate internal resources responsible for gathering and policy-based dissemination of cybersecurity and threat intelligence that facilitate evaluation and response measures. FINRA strongly encourages firms to reconsider previous decisions not to engage in threat-information sharing forums, especially given the Federal Trade Commission and Department of Justice's April 10, 2014, policy statement explaining that cyberthreat information sharing is not likely to raise antitrust concerns.[7]

8. Cyber Insurance: Both the SEC and FINRA indicate that insurance can be part of an effective cybersecurity risk management strategy. Yet, according to the SEC, only approximately one-half of broker-dealers and one-fifth of advisers maintain insurance for losses caused by cybersecurity incidents. An effective insurance strategy should involve: (a) for firms with insurance, periodic review of coverage adequacy indexed to firm risk assessment and management; and (b) for firms without insurance, market evaluation to determine if there is available coverage that would assist in management of the financial impact of a security breach.

Conclusion

There should now be no doubt that both the SEC and FINRA are serious about the need for comprehensive cybersecurity programs. Recognizing that there is no one-size-fits-all solution, both agencies contemplate (and expect) information-driven risk management decisions, providing firms with an opportunity to craft a cybersecurity program that is custom fit to their data and physical assets, threat landscape and risk appetite. And, while there is opportunity for thoughtful assessment and improvement, one thing is clear: Firms can no longer stand by and do nothing. They all must grapple with and address the reality that cybersecurity is part of the modern business model, as well as the overall enforcement landscape.

Mark Mermelstein co-leads Orrick Herrington & Sutcliffe LLP's Cybersecurity & Data Privacy practice and is a partner in its White Collar & Corporate Investigations group in Los Angeles.

Aravind Swaminathan co-leads Orrick Herrington & Sutcliffe's Cybersecurity & Data Privacy practice and is a partner in its White Collar & Corporate Investigations group in Seattle.

Daniel J. Dunne is a member of Orrick Herrington & Sutcliffe's Cybersecurity & Data Privacy practice and is a partner in its Securities Litigation, Investigations & Enforcement practice group in Seattle.

Antony P. Kim co-leads Orrick Herrington & Sutcliffe's Cybersecurity & Data Privacy practice and is a partner in its Antitrust & Competition practice group in Washington.

[7] FTC & DOJ, *Antitrust Policy Statement on Sharing of Cybersecurity Information* (Apr. 10, 2014), *available at* https://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf (13 PVLR 653, 4/14/14).