BRYAN CAVE
A Broader Perspective
Bulletin

Securities Litigation & Enforcement Client Service Group and
Data Privacy & Security Team

To: Our Clients and Friends February 12, 2015

FINRA Publishes its 2015 "Report on Cybersecurity Practices"

On February 4, 2015, FINRA published its report on cybersecurity practices arising out of its 2014 targeted examination of firms' cybersecurity preparedness (hereinafter the "Report").[1] The Report reflects FINRA's risk management-based approach to cybersecurity issues, identifying principles and "effective practices" for member firms to consider, as opposed to decreeing specific requirements, policies or procedures. FINRA characterizes its intent in preparing the Report as an attempt to focus firms on a "risk management-based approach to cybersecurity" that can be tailored to each firm's particular circumstances.

FINRA's Report provides general guidance in eight areas that FINRA expects all firms to consider in connection with developing their respective cybersecurity programs. These eight areas are as follows:

1. Governance and Risk Management for Cybersecurity;
2. Cybersecurity Risk Assessment;
3. Technical Controls;
4. Incident Response Planning;
5. Vendor Management;
6. Staff Training;
7. Cyber Intelligence and Information Sharing; and
8. Cyber Insurance.

[1] FINRA's Report follows one day after the SEC's Office of Compliance Inspections and Examination (OCIE) published its own Risk Alert related to cybersecurity issues. OCIE's Risk Alert provides a statistical analysis of examined firms' preparedness and controls for responding to cyber threats. It can be accessed online.

Governance and Risk Management for Cybersecurity

In the Report, FINRA encourages firms to establish and maintain governance frameworks for the management of cybersecurity risks and related controls appropriate to a member firm's size and nature of its risk. The framework should support informed decision-making within the organization – at the appropriate levels of the organization – as well as a defined process for escalation of cybersecurity threats and incidents. Importantly, FINRA identifies a number of practices that it deems effective in this regard:

- Adoption of a governance framework supportive of decision-making based on a firm's specific risk tolerance;
- Involvement of senior management and, as appropriate, the firm's board on cybersecurity issues;
- Identification of specific operational frameworks and standards, which may be derived from general, publically available resources such as:
    - The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.0;[2]
    - NIST, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Revision 4;[3]
    - International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Information Technology 27001 and 27002 Framework;
    - ISACA's Control Objectives for Information and Related Technology (COBIT) 5;[4] and
    - Payment Card Industry Data Security Standard (PCI DSS).[5]

Nearly 90% of the firms that participated in the sweep used one or more of the NIST, ISO or ISACA frameworks or standards. Although FINRA did not endorse any particular framework or standard, it is clear that these may be a yardstick against which to evaluate each firm's approach to cybersecurity.

The Report further addressed the use of objective performance measurements in assessing firms' risk management efforts. Specifically, FINRA suggests that:

- Firms develop, implement, monitor, and update metrics (e.g., measurements of the volume of attacks, encryption coverage, security patches, or employee training) that provide visibility on performance of key aspects of the firm's cybersecurity practices;
- Firms develop thresholds that define target levels of performance for its cybersecurity programs (e.g., percentage of computers up-to-date with security patches and percentage of employees that attend cybersecurity training); and

[2] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[4] http://www.isaca.org/COBIT/Pages/default.aspx

[5] https://www.pcisecuritystandards.org

- Firms implement a governance framework that reviews and, as needed, revises these metrics and thresholds regularly.

Cybersecurity Risk Assessment

Regular cybersecurity risk assessment analyses should be conducted, including consideration of potential risks posed by third-party vendors. The Report details several practices described as "effective:"

- Identification and maintenance of an inventory of assets (i.e., computers, mobile devices, servers, databases, trading systems, etc.) authorized to access the firm's network and critical assets that should be prioritized for protection;
- Performance of comprehensive risk assessments that look at external and internal threats and prioritize recommendations to remediate risks.

FINRA specifically references each firm's obligations under Regulation S-P[6], which requires protection of customers' personally identifiable information. Databases containing this kind of data should be prioritized as a critical asset and protected accordingly.

FINRA further notes that a risk assessment program is a "key driver" in risk-management based cybersecurity programs. FINRA expects that this process would lead to changes in firms' controls to remediate risk. Those firms without a risk assessment program or with a fledgling program are of greatest concern to FINRA. The priority should be on the defining of practices and procedures intended to identify and mitigate risks.

Technical Controls

Not surprisingly, FINRA made clear that firms are expected to implement technical controls to protect firm software and hardware used to store and process data, as well as the data itself.

FINRA advocates the "defense in depth" strategy. This requires organizations to layer independent security controls throughout their technology systems. For example, a layered view may have components such as applications, perimeter, server, databases, and the data itself. Firms would apply independent security controls to each layer. FINRA again cites the ISO 27002, NIS TSP 800-53, and NIST Framework as useful guidelines for the selection of appropriate technical controls.

FINRA goes on to provide effective controls in the areas of 1) identity and access management (i.e., who has access, how, and for how long); 2) encryption; and 3) penetration tests (simulated attacks on a firm's systems with the intention of identifying security weaknesses).

[6] http://www.sec.gov/rules/final/34-42974.htm

Incident Response Planning

FINRA stresses the importance of establishing policies and procedures for the escalation of cybersecurity incidents (as well as roles and responsibilities). The Report sets out a number of effective practices in this area:

- Preparation of default responses for the most likely types of incidents, such as loss of customer data, network intrusion, and malware infection;
- Regular review and incorporation of threat intelligence;
- Development of containment and mitigation strategies for various pre-identified, likely incidents;
- Adoption of plans to facilitate system and data recovery (or eradication – such as deletion of malware or disabling of breached accounts);
- Implementation of investigation and damage assessment processes;
- Preemptive preparation of communications to stakeholders (e.g., customers, regulators, law enforcement, industry information-sharing bodies);
- Conduct of simulation exercises; and
- Preparation of plans to implement client confidence measures such as credit monitoring and reimbursement to customers for any financial losses.

FINRA notes that the primary objective of incident response plans is to "provide a framework to manage a cybersecurity event or incident in a way that limits damage, increases the confidence of external stakeholders, and reduces recovery time and costs."

Vendor Management

A key area often overlooked by firms is the risk associated with third-party vendors. These vendors may be as likely a candidate for a cybersecurity attack as any member firm. The Report notes that firms are expected to manage cybersecurity risks that may arise across the lifecycle of a vendor relationship. The Report provides a number of effective practices:

- Perform pre-contract due diligence on service providers to identify cybersecurity practices and risks;
- Consider the use of contractual terms (e.g., non-disclosure, confidentiality, breach notification, employee access, use of subcontractors) appropriate to the sensitivity and information to which the vendor may have access (including obligations after the relationship ends);
- Perform ongoing due diligence on vendors;
- Review vendor relationships and systems as part of the firm's own risk assessment programs;
- Establish procedures to terminate vendor access after contract expiration; and
- Establish, maintain, and monitor vendor entitlements such as their level of data access and length of access for compliance with firm security standards.

FINRA notes that the firms it reviewed that had "mature" vendor management processes kept their information security teams involved in monitoring vendor controls and processes on an ongoing basis. In particular, the Report calls out the risks and challenges associated with cloud computing, such as online client account management and online statements. For these systems, firms are encouraged to involve their information security teams in the due diligence process and continued review.

Staff Training

The Report notes that many cybersecurity attacks succeed because of human error, such as failure to follow proper customer authentication protocols, downloading malware, or responding to phishing attacks. Firms are advised to tailor training programs to the needs of its particular employee population. Firms should define cybersecurity training needs requirements, identify appropriate update cycles, use interactive training with audience participation to increase retention, and develop training around loss incidents, risk assessment processes, and intelligence gathering initiatives.

In this regard, FINRA notes that 95% of firms that were reviewed deliver mandatory cybersecurity training for staff. It noted that this training typically included a combination of general awareness training and targeted training for specific staff. The Report notes that "FINRA believes that the absence of [a cybersecurity training] program exposes a firm to increased risk of successful cybersecurity attack." In short, firms should have a cybersecurity training program.

Cyber Intelligence and Information Sharing

FINRA expects firms to stay abreast of cybersecurity threats, including the sharing of intelligence among other firms. Presumably this type of communication among firms will improve identification, detection, and response to any threat. FINRA notes that firms should assign responsibility for these efforts, establish mechanisms for distributing the threat information, and participate in information sharing organizations (e.g., FS-ISAC).

In reviewing the outcome of its 2014 sweep, FINRA notes that the securities industry "can be more effective in advancing cybersecurity for the community" and encourages firms to "revisit their hesitancy to participate in information sharing bodies." In response to concerns about regulatory scrutiny, FINRA noted that although firms must ensure that information sharing conforms to regulatory requirements, the FTC and DOJ policy statement (issued April 10, 2014) on information sharing expressly stated that "cyber threat information is not likely to raise antitrust concerns and can help secure the nation's network of information and resources."[7] The sharing of aggregate data and attack descriptions is not a violation of privacy laws.

"Cyber Insurance"

"Cyber insurance" is purchased by a minority of firms but is mentioned in the Report. While perhaps a way to transfer some cybersecurity risk, FINRA's clear focus is on the identification and mitigation of risk. For firms that already have cybersecurity insurance, FINRA suggests regular analysis of the

[7] http://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf

adequacy of the coverage and alignment with risk management policies. For firms that don't have cybersecurity insurance, FINRA suggests firms evaluate the cybersecurity insurance market to determine if it would help enhance a firm's ability to manage the financial impact of cybersecurity events.

Conclusion

There is no doubt that cybersecurity is a key risk facing the financial services industry now. Accordingly, FINRA's expectation is that firms will review the Report and assess how the principles and effective practices provided therein could help build or improve cybersecurity readiness. Simply stated, FINRA expects that firm management will make development and implementation of cybersecurity risk management processes a priority.

For questions about FINRA's Cybersecurity Report and the guidelines outlined therein, or assistance with your firm's cybersecurity policies, procedures, and risk management, please speak to your Bryan Cave contact, a member of our Securities Litigation and Enforcement or Data Privacy and Security teams, or the authors of this bulletin:

Rick Kuhlman
Partner, St. Louis
314-259-2820
rick.kuhlman@bryancave.com

Jason Kempf
Associate, St. Louis
314-259-2306
jason.kempf@bryancave.com