

Guidance on Cybersecurity: What Broker-Dealers and Investment Advisers Need to Have in Place

January 30, 2017

Client Advisory

January 30, 2017 by Valentino Vasi and Brielle E. Kilmartin

[View the PDF.](#)

According to a report released by IBM Corp. in May 2016, the financial-services industry ranked third in the number of targeted cyber-attacks in 2015 in the U.S., after health care and manufacturing. According to FINRA, the most common broker-dealer cybersecurity events include malware infections, insider threats and cyber-enabled fraudulent wire-transfers. Broker-dealers and investment advisers must have policies and procedures in place to protect their information and that of customers and clients and to respond to cybersecurity incidents.

Recommended Action Items

Here are some suggested measures for implementation by investment advisers and broker-dealers:

- Appoint a Chief Information Security Officer (CISO) and be sure he/she has sufficient resources to do the job. It is very important to identify "ownership" of the cybersecurity process within your firm, and to clearly identify the role and reporting lines for each employee or consultant involved in cybersecurity.
 - Review FINRA's 2015 Report on Cybersecurity Practices, the SEC's 2015 Risk Alert and Guidance Update, FINRA's Small Firm Cybersecurity Checklist, and FinCEN's Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions.
 - Be sure you have a written asset inventory, risk assessment of the assets and an Incident Response Plan. Test the Plan.
 - Review your cybersecurity policies and procedures for employees to follow. Determine whether they have clear instructions to follow and whether the procedures include evaluations for effectiveness and reporting to the board or equivalent governing body of your firm.
 - Be sure your policies and procedures are in writing and distributed to all staff. This does not mean that you should reveal the "secret sauce" of technical controls and risk assessment to all employees, but they must be instructed in their own responsibilities.
 - Implement a rigorous training program, including testing of all personnel, regardless of job description or seniority. The majority of cyber breaches are attributable to careless employees, and ill-intentioned current or recently separated ex-employees.
-

- When onboarding a new service provider that may have access to your electronic data, perform a thorough due-diligence review, including their cybersecurity programs. Get internal cybersecurity assessment reports from vendors and other service providers. This review should be repeated at least once a year.
- Have the CISO review your budget for 2017 and determine if it allows for any penetration testing and/or expert consulting to provide reports and advice on cybersecurity initiatives and to run periodic tests.
- Use encryption protections to safeguard client information.
- Install new firewalls and logging systems, if needed. Require secure passwords and frequent password changes.

Background

On February 3, 2015, the SEC Office of Compliance Inspections and Examinations published a Risk Alert titled “Cybersecurity Examination Sweep Summary”^[1] regarding brokerage and advisory firms’ cybersecurity procedures and controls. On the same day, FINRA published a Report on Cybersecurity Practices for broker-dealers.^[2] The guidelines were based on 2014 sweep examinations of regulated firms. The regulators recommended the use of relevant industry frameworks and standards to develop a risk-based approach to cybersecurity. This approach is consistent with the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (the “NIST Framework”) that uses a flexible methodology based on specific business requirements, risk tolerances, and available resources.^[3]

Understanding the SEC and FINRA best practices guidelines is essential for broker-dealers and investment advisers to establish and enhance cybersecurity policies, procedures, and oversight processes; protect firm networks and information including client information; identify and address risk, including those associated with vendors and other third parties; and detect and manage cyber attacks.

Summary of Guidance – FINRA

FINRA’s Report relies on the NIST Framework and embraces a flexible “one-size-does-not-fit-all” approach. FINRA’s Report identifies the following key requirements, which are discussed in more detail below:

- A rigorous governance framework with strong leadership;
- Risk assessment;
- Technical controls;
- Incident Response Plan;
- Management of vendor cybersecurity risk;
- Staff training; and
- Intelligence and information sharing to protect from cyber threats.

Governance. Based on its review of broker-dealer policies, FINRA noted certain effective practices in connection with cybersecurity governance and risk-management. A firm should:

- Define a governance structure to support decision-making based on acceptable risk tolerance.

- Identify senior management with specified responsibilities for cybersecurity.
- As appropriate, provide for engagement by the firm's board of directors or equivalent governing body.
- Create written policies and procedures to address cybersecurity.
- Use metrics and thresholds to help assess the progress and effectiveness of the firm's cybersecurity governance process.
- Dedicate appropriate resources.
- Perform cybersecurity risk assessments.

Firms should consider whether to accept, mitigate, transfer (through contract and/or cybersecurity insurance), or avoid each risk identified in a governance framework. Most firms focus on mitigation, which includes the identification, selection, implementation, performance monitoring, and updating of the controls used in its cybersecurity programs.

Risk Assessment. Firms should conduct regular assessments to identify cybersecurity risks to firm assets and firm vendors. These reviews should use metrics to quantify and track implementation, effectiveness, efficiency and impact, among other aspects. Ninety-five percent of the firms FINRA reviewed in its 2014 sweep used metrics as one of their key cybersecurity performance management tools. Through risk assessment, firms can learn to make changes to prevent, correct, and control identified risks. The NIST Framework lists six risk assessment activities:

- Identify and document asset vulnerabilities;
- Review threat and vulnerability information from information-sharing forums and sources;
- Identify and document internal and external threats;
- Identify potential business impacts and likelihoods;
- Use identified threats, vulnerabilities, probabilities and impacts to determine risk; and
- Identify and prioritize risk responses.

The NIST Framework emphasizes the importance of identifying critical assets on a firm's network and maintaining strong policies to ensure that all assets are subject to centralized review and control.

Technical Controls. Firms should apply technical controls to protect software and hardware that store confidential data. FINRA recommendations include data encryption and penetration testing to safeguard sensitive information.

- **Encryption**

This is a critical piece of a firm's cybersecurity controls. It protects the confidentiality of data by ensuring that only approved users can view it. This control can be implemented at multiple levels of a defense strategy with identifiable security benefits and operational tradeoffs at each level.

Firms should ensure that portable media, including but not limited to USB drives, backup tapes and drives of portable end-user terminals such as laptops, are encrypted. There are many examples of firms losing sensitive data through the loss of portable media

and computing devices. These devices are at much higher risk of loss and theft than fixed storage media devices located in offices and data centers.

- **Penetration Testing**

Penetration tests can include external penetration checks to test a firm's systems that are exposed to the outside world, typically via the internet, and internal penetration testing to test a system's resilience to insider threats. Secret penetration tests, where only a small number of firm personnel are aware of the test, allow a firm to assess its detection and incident response controls. Open tests are done with full knowledge of system stakeholders and are focused on testing a system's preventative controls.

Penetration testing simulates attacks against a firm's computer system. The goal of this testing is to determine feasibility of potential attacks and identify vulnerabilities. Penetration tests can access the business and operational impacts of successful attacks, and check the ability of network defenders to detect and respond to attacks. They can also provide evidence to support increased investments in security personnel and technology.

Incident Response Plan. Firms should establish policies and procedures, as well as roles and responsibilities for escalating and responding to cybersecurity incidents in order to limit damage and reduce recovery time and costs. Effective Incident Response Plans include procedures for:

- Preparation of a response plan for incidents that are most likely to affect the firm;
- Containment and mitigation strategies for different types of incidents;
- Investigation and damage-assessment processes; and
- Preparation of plans for communication to customers, regulators, law enforcement, intelligence agencies, and industry information-sharing bodies.

Many firms have established a Computer Security Incident Response Team (CSIRT) responsible for receiving, reviewing and responding to computer security incident reports and activity. The most effective plans address different attack scenarios that may occur along many plausible attack paths.

Staff Training. Many cybersecurity attacks are successful because employees make mistakes like inadvertently downloading malware or being tricked by a phishing attack. Even well-meaning employees are cybersecurity risks if they are not properly trained. Employees should be informed and trained so that they understand their specific roles and responsibilities. Users should be educated on the risks associated with the data that they encounter. Firms should also consider implementing programs that combine mandatory general awareness training for all staff and targeted training for specific groups. General training should teach basic concepts such as recognizing risks, handling confidential information, password protection and mobile security. IT/management-targeted training should include application security, privilege management, emerging technology issues and software vulnerabilities.

The FINRA checklist for small firms recommends that firms assess how employees maintain devices that allow access to personally-identifiable or firm-sensitive information. A firm should identify precisely what sensitive information is stored on its systems and which employees have access to such data. If employees can access firm information remotely through portable devices, they should be properly trained to use those devices safely.

Summary of Guidance – SEC

On March 24, 2016, the SEC held a cybersecurity roundtable to discuss issues and challenges for market participants and public companies. SEC Chair Mary Jo White led the discussion. She addressed new concerns, including criminal and hired hackers, terrorists, state-sponsored intruders and misguided computer experts.^[4] The SEC noted mounting cybersecurity risks for registered investment advisers and broker-dealers.

The SEC has promulgated several regulations to promote heightened cybersecurity and identity protection initiatives. For example, Regulation S-P governs the treatment of nonpublic personal information ("NPI") about customers. It requires investment advisers and broker-dealers to notify clients about the collection, use and sharing of client NPI, and limits the disclosure of this information.

The 2015 Risk Alert assessed firm vulnerability to cyber-attacks across the financial services industry and reported on the preventative measures that had been taken. Since then, the SEC has appointed Christopher R. Hetner as Senior Advisor to the Chair for Cybersecurity Policy.^[5]

Types of Attacks. Most of the examined firms reported that they were subject to cybersecurity incidents related to malware or fraudulent emails. Over half of the firms reported receiving fraudulent emails seeking transfer of client funds, and over a quarter of those broker-dealers reported losses related to fraudulent e-mails of more than \$5,000 but less than \$75,000.

Best Practices. The SEC found that a majority of firms surveyed had adopted written cybersecurity policies and most conducted periodic audits to determine compliance with policies and procedures.^[6] Most of the broker-dealers and many of the advisers reported using metrics published by cybersecurity risk management standards like the NIST Framework.

Like FINRA, the SEC recommends that firms implement a governance and risk assessment program and implement access rights and basic controls to prevent unauthorized access to systems or information, such as multifactor authentication or updating access rights based on personnel or system changes. The SEC suggests that examiners assess the methods through which firms monitor the volume of content transferred outside the firm by employees or third parties, such as through attachments or uploads. The SEC also focused on vendor management, or practices and controls such as due diligence with regard to vendor selection, monitoring, and oversight of vendors and contract terms. Vendor relationships are considered part of a firm's ongoing risk assessment process. Firms should conduct the appropriate level of due diligence when retaining any third-party vendor.

Further Guidance. Following the Risk Alert, on April 28, 2015, the SEC's Division of Investment Management issued a Guidance Update to investment and fund advisers on improving cybersecurity. This was an advance notice of the areas that the SEC intended to look for in examinations. It was also adopted as a useful "road map" by regulated firms for their own internal reviews, evaluations, and adaptations. Since the issuance of the Guidance, many firms have added the following suggested measures to their procedures:

- **Conduct Periodic Assessments to Identify Threats and Vulnerabilities.** Firms should conduct regular assessments of:
 - The nature, sensitivity and location of information that the firm collects, processes and/or stores, and the technology systems it uses;
 - Internal and external cybersecurity threats to and vulnerabilities of the firm's information and technology systems;
 - Security controls and processes currently in place;
 - The impact, should the information or technology systems become compromised; and
 - The effectiveness of the governance structure for the management of cybersecurity risk.
- **Develop a Cybersecurity Strategy to Prevent, Detect and Respond to Threats.** This should include development and testing of an Incident Response Plan.

- **Implement the Cybersecurity Strategy Through Written Policies and Procedures and Training.** Include guidance for officers and employees.

Although the SEC's publications are "guidance," it ties cybersecurity to a firm's ability to comply with federal securities laws. The SEC expects firms to take the necessary steps to mitigate cybersecurity risk and firms are strongly advised to adopt these best practices.

Enforcement Actions

The SEC Alert and FINRA Report are guidance, not regulation. However, the SEC's Enforcement Division is using the Regulation S-P privacy rule to bring actions against firms that fail to safeguard client data.

- *In the Matter of R.T. Jones Capital Equities Management, Inc.* [\[7\]](#) The SEC brought its first enforcement action in September 2015 for a violation of Regulation S-P [\[8\]](#) against an investment adviser that was itself the victim of a security breach. Hackers stole client personally identifiable information (PII). This action made it clear that advisers cannot afford to wait until after a data breach to address cybersecurity issues. R.T. Jones, a St. Louis-based investment adviser, was charged with failing to establish required cybersecurity policies in advance of a data breach that compromised the PII of approximately 100,000 individuals. Between 2009 and 2013, the firm stored sensitive personal information of its clients on a third-party hosted web server. In 2013, the server was breached by an unknown hacker from China. According to the SEC, all of R.T. Jones' sensitive data was at risk. The firm's continued failure to adopt written policies and procedures despite SEC encouragement, failure to conduct periodic risk assessment, failure to implement a firewall or encrypt PII, and no Incident Response Plan resulted in the imposition of a penalty. The SEC and R.T. Jones agreed to a cease-and-desist order and censure, and a civil monetary penalty of \$75,000. The SEC brought this enforcement action despite the fact that the firm had not received any indication that any client had suffered financial harm as a result of the cyber-attack. The decision sends an important message, emphasizing the enforcement of Regulation S-P given the increasing occurrence of cyber attacks on financial firms.
- *In the Matter of Morgan Stanley Smith Barney LLC* [\[9\]](#) In another enforcement action brought under Reg. S-P, the SEC imposed a \$1 million penalty on Morgan Stanley in settlement of charges related to failures to protect customer information, some of which was hacked and offered for sale online. Morgan Stanley failed to adopt written policies and procedures reasonably designed to protect consumer data. An employee impermissibly accessed and transferred data regarding approximately 730,000 accounts to his personal server, which was ultimately hacked by third parties. This enforcement action illustrates the importance of extending cybersecurity measures to portable media devices like laptops that employees can access remotely.
- *In the Matter of Lincoln Financial Securities, Inc.* [\[10\]](#) FINRA has begun pursuing a more aggressive crackdown policy for cybersecurity failures. Employees of Lincoln Financial Securities, Inc. were able to access customer account details by means of shared user names and passwords. The firm did not track which or how many employees had access to the login credentials or customer data. There were no policies in place to change shared credentials when an employee left the firm or was terminated. The result was that more than a million customer account records were accessed using the shared credentials. Lincoln Financial later migrated many of its records containing customer non-public personal information to a cloud-based server but failed to ensure that the third-party cloud host had sufficient antivirus software or data encryption in place. As a result, the information of approximately an additional 5,400 customers was exposed. On November 24, 2016, a Lincoln Financial Group subsidiary agreed to pay a \$650,000 fine to FINRA to resolve allegations that it failed to protect confidential customer information from this 2012 hacking.
- On December 21, 2016, FINRA imposed \$14.4 million of fines on 12 firms, including several Wells Fargo entities, RBC Capital Markets LLC, RBS Securities, Inc., SunTrust Robinson Humphrey Inc., LPL Financial LLC, Georgeson Securities Corporation and PNC Capital Markets LLC. [\[11\]](#) The firms were disciplined for failing to keep electronic records in a particular format meant to prevent

alteration and destruction. This format, known as WORM, stands for “write once, read many” and is required for business-related electronic records under federal securities laws and FINRA rules. The format is meant to prevent alteration and destruction of such financial records. Despite the fact that no client records were modified or lost due to the failure to utilize WORM, FINRA nonetheless fined each firm for failing to maintain adequately protected electronic records.^[12]

For more information concerning the matters discussed in this publication, please contact the authors, **Valentino Vasi** (212-238-8877, vasi@clm.com) or **Brielle E. Kilmartin** (212-238-8652, kilmartin@clm.com), any member of the Carter Ledyard Cybersecurity Practice Group (**John M. Griem, Jr.**, 212-858-8659; **Melissa J. Erwin**, 212-858-8622; or **Matthew B. James**, 212-858-8644), or your Carter Ledyard relationship attorney.

Endnotes

[1] The Office of Compliance Inspections and Examinations, *Cybersecurity Examination Sweep Summary*, Volume IV, Issue 4 (February 3, 2015).

[2] FINRA, *Report on Cybersecurity Practices* (February 2015).

[3] See National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (February 12, 2014).

[4] Opening Statement at SEC Roundtable on Cybersecurity, Chair Mary Jo White (March 2014).

[5] Mr. Hetner joined the SEC in January 2015 and has more than 20 years of experience in information security and technology. He was named to his current position on June 10, 2016.

[6] In the Matter of Morgan Stanley Smith Barney LLC, Securities and Exchange Commission, Securities and Exchange Act of 1934, Release No. 78021 (June 8, 2016).

[7] In the Matter of R.T. Jones Capital Equities Management, Inc., Securities and Exchange Commission, Investment Advisers Act of 1940, Release No. 4204 (September 22, 2015).

[8] See FINRA Fines 12 Firms a Total of \$14.4 Million for Failing to Protect Records from Alteration, <http://www.finra.org/newsroom/2016/finra-fines-12-firms-total-144-million-failing-protect-records-alteration2016>.

[9] In the Matter of Morgan Stanley Smith Barney LLC, Securities Exchange Act of 1934 Release No. 78021 (June 8, 2016).

[10] FINRA Letter of Acceptance, Waiver and Consent No. 2013035036601, Lincoln Financial Securities Corporation, Respondent, Member Firm CRD No. 3870.

[11] See FINRA Letter of Acceptance, Waiver and Consent Nos. 2014043539001, 2016048685301, 2016049784101, 2016049821601, 2016050194001.

Carter Ledyard & Milburn LLP uses Client Advisories to inform clients and other interested parties of noteworthy issues, decisions and legislation which may affect them or their businesses. A Client Advisory does not constitute legal advice or an opinion. This document was not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed

herein. © 2020 Carter Ledyard & Milburn LLP.

© Copyright 2017