Morgan Lewis | White Paper

PROACTIVE APPROACH TO CYBERSECURITY:

RECENT SEC GUIDANCE AND ENFORCEMENT ACTIONS SUGGEST THAT REACTIVE FIRMS MAY BE IN THE SEC'S CROSSHAIRS

October 2015

www.morganlewis.com

INTRODUCTION

In an environment where even the largest and most powerful corporations have fallen victim to data breaches, it can be challenging to fathom how to protect against the sophisticated and ever-evolving threat of cyber attacks. The US Securities and Exchange Commission (SEC) and other regulatory law enforcers are making clear that companies, broker-dealers, financial advisers, and others must make cybersecurity—both before and after an incident—a priority.[1] The failure to take proactive measures, such as establishing and implementing written cybersecurity policies and procedures, can result in actionable conduct, even in instances without a cyber attack. When a firm experiences a data breach, not only are there significant business consequences, but the breach also increases the risk that regulators will evaluate the firm's cybersecurity policies and initiate an enforcement review.

The SEC signaled its heightened degree of scrutiny on cybersecurity preparedness by issuing its second Office of Compliance Inspections and Examinations (OCIE) Risk Alert.[2] OCIE noted that the 2015 initiative will focus more on evaluating a firm's implementation of its cybersecurity policies or procedures. This Risk Alert, combined with the SEC's past cybersecurity guidance, emphasizes the SEC's position on firms being proactive instead of reactive. Given that OCIE is intending to actually test and evaluate each examined firm's implementation of its cybersecurity systems, the findings for this round of examinations are more likely to result in significant compliance deficiencies and, potentially, enforcement actions. In light of the SEC's recent actions and public statements,[3] it is clear that cybersecurity is a concern that all firms, irrespective of size, must proactively address by developing controls and procedures reasonably designed to detect and prevent cyber attacks.

OCIE'S LATEST RISK ALERT: EXAMINER EXPECTATIONS

On September 15, 2015, OCIE announced a new round of cybersecurity examinations.[4] OCIE's second round of examinations will build on last year's findings,[5] and firms should expect a greater emphasis on their implementation of procedures and controls. The initiative will focus on, but will not be limited to, the following six areas:

- **Governance and Risk Assessment**. Examiners may assess whether firms have cybersecurity governance and risk-assessment processes relative to the areas of focus discussed below.
- **Access Rights and Controls**. Examiners may review how firms control access to various systems and data via management of user credentials, authentication, and authorization methods. This may include a review of controls associated with remote access, customer logins, passwords, and firm protocols to address customer login problems, network segmentation, and tiered access.

1. For past cybersecurity guidance, see *infra* notes 2, 6, and 18.

2. Office of Compliance Inspections and Examinations, Risk Alert: OCIE's 2015 Cybersecurity Examination Initiative (Sept. 15, 2015), *available* here ("OCIE Risk Alert - September 2015").

3. *See, e.g.,* Commissioner Luis Aguilar, Statement Before the Advisory Committee on Small and Emerging Companies (Sept. 23, 2015) (Commissioner Aguilar stated that small- and mid-sized firms must protect against cyber attacks because these firms are "not just targets of cybercrime, they are its principal target").

4. OCIE Risk Alert - September 2015, *supra* note 2.

5. For more information, see our February 2015 LawFlash, SEC and FINRA Publish Materials Addressing Cybersecurity; Office of Compliance Inspections and Examinations, Risk Alert: Cybersecurity Examination Sweep Summary (Feb. 3, 2015), *available* here.

- **Data Loss Prevention**. Examiners may assess how firms monitor the volume of content transferred outside of the firm by its employees or through third parties, such as by email attachments or uploads.
- **Vendor Management**. Examiners may focus on firm practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms. Examiners may also assess how vendor relationships are considered as part of a firm's ongoing risk-assessment process as well as how the firm determines the appropriate level of due diligence to conduct on a vendor.
- **Training**. Examiners may focus on how training is tailored to specific job functions and designed to encourage responsible employee and vendor behavior. They may also review how procedures for responding to cyber incidents under an incident response plan are integrated into regular personnel and vendor training.
- **Incident Response**. Examiners may assess whether firms have established policies, assigned roles, assessed system vulnerabilities, and developed plans to address possible future events. This includes determining which firm data, assets, and services warrant the most protection to help prevent attacks from causing significant harm.

To assist firms in assessing their cybersecurity preparedness, the Risk Alert also includes a sample request for information and documents (found here). The sample request is notably more detailed than prior guidance and provides best practices for cybersecurity policies and procedures and insight about where firms may be falling short.

CYBERSECURITY REGULATORY AND ENFORCEMENT LANDSCAPE

The cybersecurity Risk Alerts[6] suggest that the SEC is using OCIE's examination findings to determine what type of cybersecurity guidance to issue to the financial industry. The SEC and other law enforcers, however, are grappling with the need to provide regulatory guidance to put firms on notice of the applicable standards against the understanding that cybersecurity is not a "one-size-fits-all" endeavor. Possibly in recognition that cybersecurity perfection is unattainable, existing laws and regulations that used to enforce cybersecurity practices share a common theme of reasonableness. In light of the regulatory focus on cybersecurity, firms in the securities industry should be familiar with existing SEC and state regulations that are used to address cybersecurity.

Regulation S-P

Enforcement actions initiated by the SEC relating to cybersecurity are often based on violations of Rule 30 of Regulation S-P (the Safeguards Rule).[7] The Safeguards Rule requires registered broker-dealers, investment advisers, and investment companies to adopt written policies and procedures to address the administrative, technical, and physical safeguards for protecting customer records and information. Such written policies and procedures must be "reasonably designed to" do the following:

- Ensure the security and confidentiality of customer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of customer records and information.

6. *See* Office of Compliance Inspections and Examinations, Risk Alert: OCIE Cybersecurity Initiative (Apr. 15, 2014), *available* here; *supra* note 2.

7. Regulation S-P, Privacy of Consumer Financial Information, 17 C.F.R. Part 248; SEC Release No. IC-24543 (Jun. 22, 2000), *available* here. Other actions may be grounded in violations of Rule 206(4)-7 (the Compliance Rule) of the Investment Advisers Act of 1940 (the Advisers Act), or the antifraud provisions of the Advisers Act. We also note that FINRA Rule 4370 succinctly requires FINRA members to adopt a business continuity plan.

- Protect against any unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.[8]

The SEC must prove that a covered financial institution acted negligently to establish a primary violation of Regulation S-P.[9] Although an entity that violates this regulation is not subject to strict liability, the SEC has previously argued that a strict liability policy should be applied.[10] Ultimately, the SEC must "consider the totality of the circumstances . . . [and] prove by the weight of evidence that a financial institution behaved unreasonably, *i.e.*, at least negligently."[11] At this time, a firm's failure to maintain written policies and procedures that are *reasonably* designed to accomplish the regulatory objectives outlined in Regulation S-P would be sufficient grounds to enable the SEC to fine the firm. Such regulatory censure applies in cases where there was no precipitating cyber breach, but in most cases, a breach calls attention to a firm's cybersecurity policies and becomes "low-hanging fruit" for SEC enforcement review or action.

Identity Theft Red Flags Rules

SEC Regulation S-ID (also referred to as the Red Flags Rules) requires financial institutions to have *reasonable* policies and procedures for identifying relevant red flags related to identity theft, detecting those red flags, responding appropriately to red flags once detected, and updating the identity theft program on a periodic basis.[12]

Local Data Privacy Laws

Presently, 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted some form of data breach notification laws.[13] Although these laws vary by jurisdiction, they generally require covered entities (such as broker-dealers and investment advisers) to implement and maintain "*reasonable* security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[14] Most state statutes also require notification to particular parties of security breaches involving personally identifiable information. For example, New York law requires covered entities to notify the New York Attorney General, the New York State Division of State Police, and the Department of State's Division of Consumer Protection of any breaches of computerized data involving New York residents' private information.[15] In the event of a cybersecurity breach, broker-dealers and advisers should consider the applicable state laws that require notification to customers and/or reporting to government agencies.

8. 17 C.F.R. § 248.30(a)(1)-(3).

9. *See In the Matter of NEXT Fin. Grp., Inc.*, Initial Decision Rel. No. 349, Admin. Proc. File No. 3-12738, at 22 & 35 (ALJ Kelly) (Jun. 18, 2008) ("To demonstrate that a brokerage firm violated Rule 30(a), the [SEC] must: (1) require the brokerage firm to . . . provide a copy of its written safeguarding policies and procedures; (2) demonstrate through competent evidence . . . that the brokerage firm's policies and procedures were not 'reasonably designed' to accomplish the three statutory and regulatory goals; and (3) when proceeding under Rule 30(a)(3), establish through competent evidence . . . that unauthorized access 'could result in substantial harm or inconvenience to any customer'").

10. *Id*. at 22.

11. *Id*. at 23.

12. Regulation S-ID, 17 C.F.R. Part 248, Subpart C. *See also* Final Rule, Identity Theft Red Flags Rules (Apr. 10, 2013), *available* here.

13. *See* National Conference of State Legislatures, Security Breach Notification Laws (Jun. 11, 2015), *available* here.

14. *See, e.g.*, ARK. CODE ANN. § 4-110-104(b) (emphasis added); CAL. CIV. CODE § 1798.81.5(b) ("implement and maintain reasonable security procedures and practices"); and MD. CODE ANN., COM. LAW § 14-3503(a) ("implement and maintain reasonable security procedures and practices").

15. N.Y. Gen. Bus. Law § 899-aa.

Some jurisdictions also establish standards for protecting personal information.[16] For example, under Massachusetts law, companies that own or license Massachusetts residents' personal information must create and maintain a comprehensive information security program. The program must include user authentication protocols, access control measures, encryption of all data transmitted wirelessly, monitoring of systems for unauthorized access, encryption of personal information on mobile devices, firewall and malware protections, and employee training.[17]

Recent Enforcement Actions

Notwithstanding the lack of explicit cybersecurity rules, the SEC and the Financial Industry Regulatory Authority (FINRA) have sanctioned firms on numerous occasions for various cybersecurity failures in connection with the Safeguards Rule and other regulatory requirements. As depicted below, these enforcement actions involve many of the same issues discussed in the SEC's and FINRA's cybersecurity guidance and results of examination sweeps.[18] Some examples of those deficiencies include the following:

- Policies that contained only recommendations instead of mandates.[19]
- Policies that simply recited Regulation S-P and provided examples of safeguards instead of describing a firm's actual safeguards.[20]
- Failing to instruct registered representatives on how to protect customer information and how to respond in the event of a breach.[21]
- Failing to ensure that laptops were protected by encryption or other appropriate technology safeguards.[22]
- Failing to address appropriate responses to cybersecurity issues detected through branch audits.[23]

Recently, the SEC and US Department of Justice charged nine people involved in an international scheme to hack into three business newswires and steal yet-to-be published press releases containing nonpublic financial information, which was then used to make trades that generated approximately $30 million in illegal profits.[24] In another action, FINRA charged a broker-dealer with violating NASD Rules 3010 and 2110 (now FINRA Rules 3110 and 2010, respectively) by failing to comply with its written procedures requiring quarterly reviews of its internal computer systems and privacy protections.[25] FINRA noted that

16. Firms with offices or branches located overseas should consider the implications of those jurisdictions' legal obligations.

17. *See generally,* 201 C.M.R. § 17.00.

18. *See* Financial Industry Regulatory Authority, Report on Cybersecurity Practices (Feb. 2015), *available* here; Office of Compliance Inspections and Examinations, Risk Alert: Cybersecurity Examination Sweep Summary (Feb. 3, 2015), *available* here.

19. *In the Matter of LPL Fin. Corp.*, Exchange Act Release No. 58515, Admin. Proc. File No. 3-13181, at 4 (Sept. 11, 2008) (finding that a firm violated the Safeguards Rule), *available* here.

20. *In the Matter of Marc A. Ellis*, Exchange Act Release No. 64220, Admin. Proc. File No. 3-14328, at 3 (Apr. 7, 2011) (finding that a former COO aided and abetted a firm's violation of the Safeguards Rule), *available* here.

21. *Id.*

22. *In re Wells Inv. Sec. Inc.*, Letter of Acceptance, Waiver and Consent No. 2009019893801, at 10 (Nov. 22, 2011) (finding that the firm violated the Safeguards Rule and NASD Rule 3010 (predecessor to FINRA Rule 3110)).

23. *In the Matter of Commonwealth Equity Services, LLP*, Exchange Act Release No. 60733, Admin. Proc. File No. 3-13631, at 2 (Sept. 29, 2009) (finding that the firm violated the Safeguards Rule), *available* here.

24. For more information, see our September 2015 LawFlash, SEC and DOJ Hacking Prosecutions Highlight SEC's Increased Interest in Cybersecurity Risks.

25. *In re Tradewire Sec., LLC*, Letter of Acceptance, Waiver and Consent No. 2009015980301, at 6 (Dec. 14, 2012), *available* here.

if the firm had enforced these quarterly reviews, it would have discovered its failure to install essential monitoring software in at least 19 employees' computers.[26]

The Federal Trade Commission (FTC) is also taking an aggressive role in reviewing whether a company has an adequate cybersecurity program. In the recent *FTC v. Wyndham Worldwide* decision, the US Court of Appeals for the Third Circuit upheld the FTC's authority to enforce a claim for unfair practices. The FTC had, inter alia, alleged that the company, which experienced three cyber attacks resulting in a theft of consumer data, had not used commercially reasonable methods for protecting consumer data and overstated its cybersecurity protections in its published privacy policy.[27] The decision recognizes the FTC's authority to bring enforcement actions for what it deems are "unfair cybersecurity practices." *Wyndham Worldwide* illustrates how companies' inability to adequately protect valuable and sensitive confidential and customer information may result in an enforcement action.

These enforcement actions indicate the SEC's and other regulatory agencies' willingness to use existing regulations to ensure the security of customer information. The common theme is that each of these actions was commenced *after* an alleged data breach. Despite these firms being the victim of a cyberattack, regulators are scrutinizing the types of actions that firms *could have taken* to thwart the attack and sanctioning firms for having unreasonable cybersecurity policies and procedures, or a lack thereof. In the face of this heightened scrutiny, registered brokerage and advisory firms should ensure that they take a proactive stance and implement effective cybersecurity practices and policies as an ongoing operational matter.

PRACTICAL IMPLICATIONS—WHAT CAN YOU DO?

With Regulation S-P as a starting point and the OCIE cybersecurity guidance, the SEC appears to be moving toward a principles-based risk-management regime. Although there may be no perfect security system in the face of an ever-evolving threat, the existing regulatory framework couches cybersecurity in the language of risk management. Weighing costs and benefits and calibrating risk appetites should be familiar to organizations. In that vein, a firm's cybersecurity protocols should emphasize the actions taken *when*, not *if*, a cybersecurity breach occurs. Organizations should consider taking the following preventative measure:

- Prepare for hard-hitting examinations by taking appropriate measures, such as those described herein, to review existing cybersecurity policies in advance of an examination. OCIE's recent Risk Alert places an emphasis on a firm's *implementation* of policies and procedures instead of merely *having* policies and procedures.
- Tailor cybersecurity policies and procedures to address your firm's risk appetite and to address and mitigate cyber risks. By doing so, firms that are notified of regulatory enforcement action will have stronger arguments that their policies were reasonably designed to prevent or mitigate against cybersecurity threats.
- Implement appropriate oversight and review protocols. Cybersecurity is increasingly an enterprisewide concern that needs to start at a firm's board of directors and permeate throughout the organization. Firms can no longer view cybersecurity as issues confronting only compliance or information technology departments.

---

26. *Id.*

27. *F.T.C. v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015), ("*Wyndham Worldwide*") *available* here. FTC Chairwoman Edith Ramirez noted that the Third Circuit's "decision [in Wyndham] reaffirms the FTC's authority to hold companies accountable for failing to safeguard consumer data. It is not only appropriate, but critical, that the FTC has the ability to take action on behalf of consumers when companies fail to take reasonable steps to secure sensitive consumer information." Statement of FTC Chairwoman Edith Ramirez on Appellate Ruling in the Wyndham Hotels and Resorts Matter (Aug. 24, 2015), *available* here.

  - Ensure that directors understand the legal implication of cyber risks as they relate to their firm's specific circumstances.
  - Document board minutes and briefing materials related to cybersecurity. If a firm has not already incorporated cybersecurity into its overall governance structure, it should do so and ensure that the board of directors is involved in cybersecurity discussions and is updated on risk assessments and other measures that the firm takes related to cybersecurity preparedness.
  - Monitor internal training and controls, and provide regular training to new and existing employees with respect to cybersecurity and the protection of customer data, including personally identifiable information. In light of recent headlines involving the firing of a Vanguard employee who allegedly blew the whistle on Vanguard's cybersecurity policies,[28] training employees and maintaining strong policies and procedures with escalation procedures are especially important to prevent threats of whistleblowers who believe that a firm has lax security protocols.
- Become familiar with reporting obligations pursuant to, for example, Regulation S-ID, state reporting requirements, and FINRA rules.[29] Identify the various requirements in an incident response plan to accurately and timely respond to such cybersecurity situations.
- Monitor vendor relationships by reviewing agreements with third-party vendors or service providers to ensure that these agreements contain provisions related to cybersecurity. Even agreements entered into just a few years ago should be reviewed for compliance with a firm's cybersecurity efforts. For agreements that do not incorporate cybersecurity provisions, firms should renegotiate these agreements. A weak link outside of the firm undermines all of its cybersecurity efforts.
- Prepare and regularly test the incident response plan. Take steps to ensure that the plan will work when it is needed.
- Conduct routine risk assessments that identify cybersecurity exposures and specific vulnerabilities, then modify policies or procedures to reflect the outcome of the risk assessment. Firms should conduct periodic risk assessments to gain a deeper understanding of the types of risks to which they are exposed and the likelihood of the risks arising in the future.
  - FINRA has stated that asset inventories are a "key component" of a risk assessment and that a risk assessment requires a firm to know "what assets they have, what assets are authorized to be on their network and what assets are most important to protect."[30]
- FINRA and, in our experience, other financial regulators, recommend that firms enroll in data-sharing programs related to cybersecurity. For example, firms should consider whether to participate in the Financial Services Information Sharing and Analysis Center's program.

CONCLUSION

Cybersecurity issues will continue to be at the forefront of regulators' concerns. Firms must be proactive to address cybersecurity risks and implement written policies and procedures reasonably designed to address such risks. As more valuable information migrates online and firms innovate more ways of

28. Joe Morris, Vanguard Fires Cyber-Security Whistle-Blower, *Ignites* (Sept. 21, 2015).

29. FINRA Rule 4530(b) imposes reporting obligations on member firms. *See also* FINRA Regulatory Notice 11-06 and 11-32 for additional information on Rule 4530(b) filing requirements as well as the Rule 4530 Reporting Requirements FAQ.

30. Report on Cybersecurity Practices (Feb. 2015), *supra* at note 18.

interacting with clients and develop information-sharing techniques, the challenge of addressing cybersecurity will only increase.

Contacts

If you have any questions or would like more information on the issues discussed in this White Paper, please contact any of the following Morgan Lewis lawyers:

Silicon Valley
Mark L. Krotoski +1.650.843.7212 mkrotoski@morganlewis.com

Boston
Carmen C. Chan +1.617.951.8807 carmen.chan@morganlewis.com

Chicago
Merri Jo Gillette +1.312.324.1134 mgillette@morganlewis.com
Sarah V. Riddell +1.312.324.1154 sriddell@morganlewis.com

San Francisco
Susan Resley +1.415.442.1351 sresley@morganlewis.com
W. Reece Hirsch +1.415.442.1422 rhirsch@morganlewis.com

Philadelphia
Gregory T. Parks +1.215.963.5170 gparks@morganlewis.com

About Morgan, Lewis & Bockius LLP

Founded in 1873, Morgan Lewis offers nearly 2,000 lawyers—as well as patent agents, benefits advisers, regulatory scientists, and other specialists—in 28 offices across North America, Europe, Asia, and the Middle East. The firm provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.