ALSTON&BIRD

CYBER ALERT

A Publication of the Cybersecurity Preparedness & Response Team

WWW.ALSTONPRIVACY.COM DECEMBER 17, 2015

Effective Cybersecurity: The Evolving Regulatory Landscape for Investment Advisers, Investment Companies and Broker-Dealers

By Kim Peretti and Jason Wool

Cybersecurity has become a top concern for executives and boards across all sectors of commerce and critical infrastructure that rely on digital technologies—including financial services—and investment advisers, investment companies and broker-dealers ("market participants") fall squarely within that group. Over the last two years, regulators have increasingly set their sights on this group, which is being subjected to increasingly rigorous scrutiny both as part of examinations and through enforcement actions.

The Securities and Exchange Commission (SEC) implemented the so-called Safeguards Rule, which is part of Regulation S-P, pursuant to the Gramm-Leach-Bliley Act in 2000. In December 2004, the SEC updated the Safeguards Rule to require that safeguarding policies and procedures be written, which became effective on July 1, 2005. The SEC was not particularly active in enforcing the rule for several years thereafter.

The Safeguards Rule requires registered investment advisers, investment companies and registered broker-dealers to establish written policies and procedures reasonably designed to (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

The Regulatory Environment

The SEC Office of Compliance Inspections and Examinations (OCIE) has significantly increased its interest in data security issues in recent years. OCIE has gone from mentioning in its 2013 examination priorities statement that it "may conduct examinations" on cybersecurity topics to conducting a targeted cybersecurity examination sweep of more than 100 registered investment advisers and broker-dealers in 2014, with a second round of cybersecurity examinations recently announced in September 2015.[1] The Financial Industry Regulatory Authority (FINRA), a self-regulatory organization (SRO) that creates and enforces rules for broker-dealers, also conducted a set of targeted sweeps in 2014 before issuing detailed guidance on data security early in 2015.

---

1 SEC, "OCIE's 2015 Cybersecurity Examination Initiative," *National Exam Program Risk Alert*, Sept. 15, 2015 ("OCIE Alert").

Taken together, the OCIE's and FINRA's publications on data security form a detailed outline of their potential expectations for market participants, which may inform the examinations they conduct.[2] These expectations cover a range of topics, including governance and risk management/assessment, access management, data loss prevention, patch management, vendor management, training, incident response, network/data monitoring and protection, threat intelligence/information sharing, cyber insurance and more.

The SEC and FINRA have also initiated numerous enforcement actions arising from data security lapses, primarily arising out of the Safeguards Rule and the requirement to implement a supervisory system for compliance with it and other security-related regulations.[3] These enforcements also help to highlight regulatory expectations, as they indicate bases for subject violations such as:

- Inadequate security policies
- Inadequate or improper implementation of security policies
- Inadequate evaluation of security controls
- Inadequate enhancement of controls promptly after a known threat or risk
- Password vulnerabilities
- Failure to remediate known application vulnerabilities
- Lack of a responsible senior officer for data security
- Inadequate steps following a security incident
- Inadequate use of antivirus software
- Inadequate use of encryption for sensitive records
- Inadequate use of firewalls
- Inadequate training and failure to review incident logs
- Failure to have an intrusion prevention/detection system
- Inadequate controls over shared accounts
- Inadequate and misleading customer notifications of an incident
- Inadequate monitoring of vendors

---

2 OCIE's examinations "seek to determine whether the entity being examined is: conducting its activities in accordance with the federal securities laws and rules adopted under these laws …; adhering to the disclosures it has made to its clients, customers, the general public and/or the Commission; and implementing supervisory systems and/or compliance policies and procedures that are reasonably designed to ensure that the entity's operations are in compliance with the applicable legal requirements." SEC, Examination Information for Entities Subject to Examination or Inspection by the Commission.

3 Other regulations subject to supervision requirements include Regulation S-ID, the "Identity Theft Red Flags Rules," as well as a variety of SEC regulations that are not explicitly security related but could be violated by a data or cybersecurity incident, such as those addressing fraud, business continuity and the ability to process shareholder transactions. *See* DIM, "Cybersecurity Guidance," Guidance Update No. 2015-02, Apr. 2015, at 2.

Most recently, the SEC sanctioned an investment adviser under the Safeguards Rule for failing to protect the sensitive personal information of its clients on a compromised third-party hosted web server despite there being no evidence of access or acquisition of the data or of any harm to the affected clients.[4] Of primary concern to the SEC was the investment adviser's failure to adopt written policies and procedures reasonably designed to protect customer records and information. Thus, despite the fact that the Safeguards Rule is relatively brief and nondescript, it potentially covers a broad range of conduct, and the recent enforcement action signals that the SEC is unafraid to pursue sanctions even in the absence of harm to individuals.

The 2015 enforcement and other recent actions show that the regulators expect market participants to have substantial engagement with cybersecurity issues as part of their compliance efforts. One overarching topic that has received particular attention is security risk management. In a guidance update issued in April 2015, the SEC's Division of Investment Management (DIM) noted that "[c]yber attacks on a wide range of financial services firms highlight the need for firms to review their cybersecurity measures" and described "a number of measures that funds and advisers may wish to consider in addressing cybersecurity risk."[5] These measures include conducting periodic risk assessments; creating a strategy to prevent, detect and respond to cybersecurity threats, including through a variety of technical access controls, data encryption, data loss prevention techniques, data backup and retrieval, and the development and testing of an incident response plan; and implementing this strategy through written policies and procedures, training and compliance monitoring.[6]

Cybersecurity Preparedness: Six Practical Steps

Market participants have gone from being historically subject to a vague, generic obligation to safeguard customer data to now having to comply with broad and relatively detailed expectations from the SEC and/or FINRA for data security. Beyond that, those cybersecurity requirements are now backed by a demonstrated willingness to engage in enforcement actions when entities fall short—even when customers are not actually harmed. These expectations have emerged mostly in the last two years, creating some uncertainty as to whether a particular cybersecurity program is sufficient and appropriate.

Fortunately, the SEC's and FINRA's publications and enforcement actions provide market participants with guidance on effective cyber risk mitigation and how to build an adequate and defensible program. Below are six activities market participants can engage in to assist with their organizations' cybersecurity preparedness and address several of the SEC's and FINRA's communicated expectations and recommendations:

1. **Conduct a Cyber Risk Assessment.** The SEC and FINRA have emphasized risk assessments as a recommended risk management tool.[7] Market participants can assess their cyber risk by identifying the threats to and vulnerabilities of their systems and the likely impact of a successful compromise. Once specific risks are identified, controls specifically geared towards mitigating those risks can be designed and implemented. For instance, high risk data could be encrypted and stored on a network location that is strictly access controlled for safekeeping. This process can be repeated regularly to ensure that new or modified threats and

---

4 *See* Investment Advisers Act of 1940 Release No. 4204, Admin. Proc. File No. 3-16827 (Sept. 22, 2015) ("2015 Enforcement").

5 *See* DIM Guidance at 1.

6 *Id.* Risk management is also addressed at length in FINRA's *Report on Cybersecurity Practices*, as well as in both of the SEC's Risk Alerts concerning its cybersecurity examination initiatives.

7 *See e.g.,* DIM Guidance at 1-2; OCIE Alert at 5; FINRA, "Report on Cybersecurity Practices" at 12-15 (Feb. 2015) ("FINRA Report").

vulnerabilities are incorporated into this calculus. Entities can also assess the effectiveness of the governance structure associated with this process, such as the communication of significant risks to senior management.

2. **Enterprise Security Assessment.** The SEC and FINRA have communicated a number of recommended practices, either through guidance or enforcements. In addition, they have identified the use of frameworks or standards (or parts thereof) as being potentially beneficial as reference points.[8] Market participants can conduct a formal review of their security practices against identified benchmarks (including SEC and FINRA guidance). Using the results of this assessment, market participants can identify risks arising from gaps as well as strategies for mitigating them in a prioritized, risk-informed manner.

3. **Vendor Risk Management Review.** As service providers and other vendors have been recognized in recent years as particularly effective attack vectors for bad actors—a risk the SEC and FINRA have specifically identified as being a significant concern—managing cybersecurity risks with regard to these third parties has become an essential exercise. Market participants may wish to assess their vendors' cybersecurity practices, as well as their vendors' access and connectivity to their own networks and data, and review relevant contracts to assess how they address data security. Market participants may also wish to revise contract templates to address security issues more robustly in future engagements.

4. **Data Breach Response Plan Development/Improvement.** The SEC and FINRA have identified incident response preparedness as an important element of cyber due diligence.[9] Market participants should be sure to develop and document an effective, security-oriented incident response plan that covers the technical and business sides of responding to a security incident based on their organization's risk profile and relevant regulatory and industry requirements and guidance.

5. **Tabletop Exercises.** Likewise, market participants should test their incident response plans through tabletop exercises and breach simulations.[10] These exercises should walk through the full lifecycle of a breach response. Following the exercise, market participants may wish to incorporate lessons learned from the simulation and reissue its response plan.

6. **Education and Training.** Both the SEC and FINRA have emphasized training and education as important steps in implementing cyber risk management strategies.[11] Market participants may wish to initiate in-depth training and educational initiatives focused on data security and common attack vectors and pitfalls to help prevent human-focused attacks such as social engineering and phishing, as well as to engrain a culture of security within their organizations. These initiatives should specifically include and target senior executives, whose buy-in and compliance may be particularly important in ensuring that security mindfulness trickles down to the rest of the organization.

As the SEC initiates its next round of cybersecurity sweeps, it is never too late for market participants to make sure their organizations' cyber health is up to snuff from a legal perspective.

---

8 *See e.g.,* FINRA Report at 8-10; DIM Guidance at n. 13.

9 *See e.g.*, DIM Guidance at 2; OCIE Alert at 3, 5; FINRA Report at 23-25.

10 *See e.g.,* OCIE Alert at 5; FINRA Report at 23.

11 *See e.g.,* DIM Guidance at 2; OCIE Alert at 2, 4-5; FINRA Report at 31-33.

If you have any questions or would like additional information, please contact Kimberly Peretti, Jim Harvey or Jason Wool.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com