The Investment Lawyer
Covering Legal and Regulatory Issues of Asset Management
VOL. 27, NO. 5 • MAY 2020

REGULATORY MONITOR

SEC Update

By Elizabeth Gray, Daniel Alvarez, Elizabeth Bower, and Marc Lederer

SEC Office of Compliance Inspections and Examinations Issues Observations on Cybersecurity and Resiliency Practices

In January 2020, the US Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) published "Cybersecurity and Resiliency Observations"[1] (the Release). The Release reinforces the Securities and Exchange Commission's (SEC) position that cybersecurity risk management is a priority for the agency and an essential component of compliance by market participants such as broker-dealers, investment advisers, clearing agencies, and national securities exchanges. The Release summarizes OCIE's observations of industry practices and approaches to managing cybersecurity risk collected during thousands of examinations of such regulated entities.

Recognizing that there's no such thing as a "one-size-fits-all" approach to cybersecurity, the Release nevertheless is designed to provide market participants with a detailed framework for evaluating their own cybersecurity programs. While the SEC previously has instituted enforcement actions relating to cybersecurity programs, the Release signals a willingness by the SEC to engage in discussions with regulated entities through OCIE examinations regarding those programs and suggests that market participants should reevaluate their cybersecurity programs against OCIE's observations to enhance cybersecurity preparedness and operational resiliency.

What follows is a summary of OCIE's observations on cybersecurity practices and approaches.

Governance and Risk Management

OCIE observes that corporate governance remains an essential component of an acceptable cybersecurity program, and effective cybersecurity programs begin with senior leaders who are committed to improving their organization's cyber posture. The Release notes that the key elements of an effective governance and risk management program generally include: (1) involving appropriate board and senior leadership in setting the strategy of and overseeing the organization's cybersecurity and resiliency programs; (2) a risk assessment to identify, analyze, and prioritize cybersecurity risks to the organization; (3) written cybersecurity policies and procedures to address those risks; and (4) the effective implementation and enforcement of those policies and procedures. Such policies and procedures are comprehensive, addressing areas such as (1) access rights and controls; (2) data loss prevention; (3) mobile security; (4) incident response and

resiliency; (5) vendor management; and (6) training and awareness. Cybersecurity policies and procedures are tested and monitored on a regular, frequent basis and are continuously evaluated and adapted to changes. Such policies and procedures are communicated in a timely manner to decisionmakers, customers, employees, other market participants, and regulators as appropriate.

Access Rights and Controls

Access rights and controls determine who the appropriate users for an organization's systems are and limit access to those users. Access is limited to sensitive systems and data, based upon the users' need to perform legitimate and authorized activities on the organization's information systems. User access is managed through means such as multifactor authentication and re-certification of users' access rights. Access is immediately revoked for individuals no longer employed by the organization, including former contractors. Failed log-in attempts and account lockouts as well as anomalous or unusual customer requests are monitored and investigated.

Data Loss Prevention

Data loss prevention includes a set of tools and processes an organization uses to ensure that sensitive data, including client information, is not lost, misused, or accessed by unauthorized users. Such tools include: (1) vulnerability scanning; (2) perimeter and detective security; (3) patch management; (4) taking inventory of hardware and software; (5) encryption and network segmentation; (6) insider-threat monitoring; and (7) securing legacy systems and equipment.

Mobile Security

Policies and procedures are established for the use of mobile devices. Employees are trained on mobile device policies and procedures. A mobile device management application or similar technology is used. Security measures are implemented on mobile devices, including multifactor authentication.

Incident Response and Resiliency

Incident response plans are written and involve: (1) the timely detection and appropriate disclosure of material information regarding incidents; and (2) assessing the appropriateness of corrective actions taken in response to incidents. These plans address applicable reporting requirements, such as determining whether an incident should be reported to any affected individuals, regulators, the FBI, and local authorities, and whether certain filings need to be made, such as a suspicious activity report (SAR) or a disclosure on a public filing. These plans designate employees with specific roles and responsibilities in the event of a cyber incident. The plans are tested using a variety of methods, including tabletop exercises. Determinations are then made regarding whether the plan should be updated.

An important part of these plans is how quickly the organization recovers and again safely serves clients following an incident. The Release notes that resiliency efforts include: (1) identifying and prioritizing core business services; (2) understanding the impact of an incident on business services; (3) maintaining backup data; and (4) considering cybersecurity insurance.

Vendor Management

OCIE observes that vendor management programs are established to ensure that vendors meet security requirements and that appropriate safeguards are implemented. Policies and procedures are implemented to: (1) conduct due diligence on vendors; (2) monitor and oversee vendors, and the contract terms with such vendors; (3) assess how vendor relationships are considered a part of the organization's ongoing risk assessment process as well as how the organization determines the appropriate level of due diligence to conduct on a vendor; and (4) assess how vendors protect any accessible client information.

Training and Awareness

Organizations train employees on cyber risks and responsibilities. Training programs consist of

written policies and procedures, effective training exercises and monitoring to determine the effectiveness of training for potential updating.

Key Takeaways

As the SEC and OCIE treat cybersecurity as a priority for regulated entities, we recommend review of the Release and to consider incorporating the highlighted components into cybersecurity programs. Indeed, regulated entities should be reminded that an effective cybersecurity program is necessary in order to comply with various SEC rules and regulations, including the safeguarding rules in Regulation S-P,[2] the disclosure requirements in Regulation S-K and Regulation S-X,[3] the disclosure controls and procedures of Exchange Act Rules 13a-15 and 15d-15,[4] the insider trading prohibition,[5] and the disclosure obligations under Regulation FD.[6]

Ms. Gray, **Mr. Alvarez**, and **Ms. Bower** are partners at Willkie Farr & Gallagher LLP in Washington, DC. **Mr. Lederer** is a staff attorney at Willkie Farr & Gallagher LLP in New York, NY.

NOTES

1 OCIE Cybersecurity and Resiliency Observations.
2 17 CFR Part 248, Subpart A, and Appendix A to Subpart A.
3 17 CFR part 229; 17 CFR Part 210.
4 17 CFR 240.13a-15; 17 CFR 240.15d-15.
5 17 CFR 240.10b5-1.
6 17 CFR 243.100.