Proskauer

OCIE Publishes Cybersecurity and Resiliency Observations

February 6, 2020

Background

On January 27, 2020, the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") published its Cybersecurity and Resiliency Observations. Cybersecurity and data protection for market participants have been key focuses of OCIE for several years. These observations provide useful insights into OCIE's examination priorities in these areas. OCIE compiled these observations by observing industry practices during examinations of investment advisers, broker/dealers and other registrants. The report notes that there is "no such thing as a 'one-size fits all' approach" to cybersecurity preparedness, but that the observations might factor into "their consideration of how to enhance cybersecurity preparedness and operational resiliency." The report details seven specific areas of focus.

Areas of Focus for OCIE

- *Governance and Risk Management*. It is important for senior leaders to advocate and prioritize cybersecurity programs in order to set the right tone throughout the firm. Further, OCIE recommends risk assessments to identify cybersecurity risks (including identifying and prioritizing potential vulnerabilities, such as remote or traveling personnel, insider threats, international operations and other geopolitical risks), as well as written policies and procedures and for those written policies and procedures to be actually implemented and enforced. OCIE also indicated that effective cybersecurity programs and policies should be continuously tested, evaluated and adapted.
- *Access Rights and Controls*. Access to sensitive data should be specifically controlled and limited based on the user's legitimate business needs to access such data and should be especially limited during onboarding, transfers and terminations. Further, strong passwords and multi-factor authentication (if applicable) should be required to access sensitive data. Firms also should implement a separation of duties for user access approvals, and users' approvals to specific sensitive data should be re-certified on a periodic basis. In addition, access to accounts (including failed login attempts, account lockouts, and requests for

username/password changes) should be monitored. Finally, OCIE recommends that firms revoke access to data and systems in a timely matter for personnel who no longer need access, including former contractors and individuals who are no longer employed.

- *Data Loss Prevention*. Firms should take steps to ensure that sensitive date is protected and maintained. This can be achieved by establishing mechanisms that (i) prevent external access (including firewalls, email security systems and web proxy systems), (ii) detect unauthorized attempts to access data (including signature and behavioral-based capabilities that can identify incoming fraudulent communications) and (iii) proactively scan for any vulnerabilities in the data systems. Firms also should utilize encryption to protect data and maintain an inventory of all of the firm's hardware and software assets to ensure that protection is universal. In addition, firms should establish procedures to ensure that sensitive data is identified and blocked before it is transmitted via an unsecure mechanism (*e.g.*, account numbers, social security numbers, and trade information). Finally, OCIE suggested that firms should establish procedures for decommissioning hardware to ensure that sensitive information is removed before disposal.
- *Mobile Security*. OCIE is focused on the unique cybersecurity risks posed by mobile devices. Firms should establish explicit policies and procedures for use of mobile devices, and personnel should receive training regarding those policies and procedures. Firms also should implement multi-factor authentication and ensure that they have appropriate policies in place if personnel access firm systems on their personal devices. Finally, firms should be able to remotely clear or delete data from a mobile device.
- *Incident Response and Resiliency*. Firms should have a plan in place in the event of a data breach, which should include guidelines on the planned response to a variety of scenarios (including denial of service attacks, malicious disinformation, ransomware and other scenarios) and notification and communication procedures, including any reporting requirements associated with a cyber incident. Reporting requirements might include contacting local authorities or the FBI in the event of an attack, informing regulators, and notifying customers or clients of a cyber event. In addition, personnel should be trained to execute the response plan and should have well-defined roles in case of a cyber incident. Finally, firms should identify core business systems and processes and consider putting in place auxiliary systems or additional data back-ups.
- *Vendor Management*. Firms should have a specific program in place to ensure that all third-party vendors are carefully selected and overseen, that all cybersecurity requirements are met, and that contract terms with vendors reflect those requirements. This can be achieved by using questionnaires and/or independent

audits and by establishing procedures for onboarding, terminating, and replacing vendors. OCIE also expects that firms will consistently reassess vendor relationships in the context of firm-wide cybersecurity risk assessments.

- *Training and Awareness*. Effective training programs are an important component of a firm's cybersecurity program and should make personnel aware of cybersecurity threats to the firm. Firms should conduct trainings that use specific cybersecurity examples in order to best prepare personnel for a wide range of cyber incidents. Trainings should routinely be reevaluated and upgraded to respond to developments with respect to the firm and new cyber threats.

Action Items

OCIE recommends that all market participants review their cybersecurity policies and practices and assess their level of preparedness.

Note that the recommendations in the report are neither mandatory nor exhaustive. Each firm should address cybersecurity and resiliency based on its own size, resources and other factors.

Related Professionals

- **Christopher M. Wells**