Blogs
January 29, 2020
OCIE Releases New Observations on Cybersecurity and Resiliency

On January 27, 2020, the Office of Compliance Inspections and Examinations ("OCIE") of the U.S. Securities and Exchange Commission ("SEC") released observations on cybersecurity and resiliency (the "Observations"). In them, OCIE presented several key cybersecurity issues that industry participants should seek to address such as the construction and implementation of a comprehensive cybersecurity program, the prevention of unauthorized access to systems, the theft of information, responding to cyber incidents, and vendor management. In doing so, OCIE highlighted elements of successful cybersecurity efforts.

OCIE's Observations

While acknowledging that each firm's cybersecurity program must necessarily be tailored to the firm, OCIE emphasized several elements commonly found in successful cybersecurity programs:

- **Governance and Risk Management:** Effective cybersecurity programs begin with engaged senior management that is committed to improving its organization's cybersecurity. Critical to governance and risk management are: 1) risk identification and analysis, 2) followed by written policies and procedures to address the risk, and 3) effective implementation and enforcement of the policies and procedures. Senior management should ensure that a cybersecurity program is comprehensive, and actively monitored, managed, and adjusted.
- **Access Rights and Data Loss Prevention:** Firms should restrict, control, and monitor the access rights to their networks and systems by tailoring each user's rights to his or her specific needs. Systemic monitoring is key to identifying suspicious behavior or unauthorized access and ensuring that suspicious activity is reported. In addition to preventing unauthorized access, firms should implement measures to prevent the unauthorized extraction of data. Such measures could include scanning for vulnerabilities in systems, encryption of data, and installing anti-virus and anti-malware.
- **Mobile Security:** Firms should have mobile device policies and procedures and implement appropriate security measures. For example, limiting and or preventing the transfer of business-related information to personal devices. Firms should be able to remotely wipe data and content from current or former employees' personal devices.
- **Incident Response:** The response starts first with timely detection and appropriate disclosure. A firm should have clear procedures for how it would respond to a cybersecurity incident, such as denial of service attacks, malicious disinformation and ransomware. These procedures should include, among other things, key employee succession plan, assignment of tasks, identification of key contacts, and maintenance of back-up data offline. Such procedures should not only include how a firm would address the threat itself, but also the systems that would allow it to remain operational for its customers during the incident. Procedures should be routinely tested and modified accordingly.
- **Vendor/Third-Party Management:** Because of the system access that vendors and other third-parties can potentially gain, firms should carefully vet vendors and continue to monitor throughout the lifecycle of any contract. Oversight should include information on each vendor's own cybersecurity efforts as well as how each vendor protects any accessible client information.
- **Training and Awareness:** Training is key as it provides relevant and timely information to personnel regarding risks and responsibilities.

Conclusion

The Observations are the most recent, but not the first indication of OCIE's and the SEC's focus on cybersecurity

issues. OCIE has included cybersecurity as a key element in its examination program over the past eight years, including for 2020, and has also published eight risk alerts related to cybersecurity. In addition, the SEC maintains a cybersecurity resource webpage. However, the Observations do serve to reemphasize OCIE's and the SEC's focus in 2020 on cybersecurity issues and provide specific issues and actions for firms to consider.

Explore more in

Investment Management