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

January 30, 2020

The SEC Office of Compliance Inspections and Examinations (OCIE) recently published observations related to cybersecurity and operational resiliency practices observed in its examinations. OCIE reiterated its continued focus on cybersecurity issues, citing eight risk alerts related to cybersecurity it has published over the last few years.[1] OCIE conducts examinations for compliance with Regulation S-P and S-ID, which apply to broker-dealers and investment advisers, and Regulation SCI, which applies to exchanges and other SCI entities. The publication provides important guidance to regulated entities about the likely subjects of SEC exams, the expectations of its examiners, and the subjects of potential enforcement referrals.

OCIE's observations are based on thousands of examinations of broker-dealers, investment advisers, clearing agencies, national securities exchanges, and other SEC registrants. Although OCIE frames the guidance as a collection of observations, the context suggests that OCIE views these approaches as good practices and issued the guidance to inform the market more broadly. In future examinations, OCIE may focus in particular on these issues.

OCIE emphasized the need for periodic re-evaluation and changes to match the evolving threat environment each organization faces, although they acknowledged that there is no "one-size fits all" approach to cybersecurity preparedness and resiliency. They also pointed to resources available to registrants to keep up to date on evolving cyber threats.

OCIE highlighted seven areas of focus:

Governance and Risk Management

OCIE noted the various governance and risk management measures that organizations use, including senior level engagement in setting the strategy and oversight of the organization's cybersecurity and resiliency programs. We believe it is significant that they began their observations with a discussion of senior leadership engagement, suggesting it may be a particular subject of future OCIE exams. Other measures include ongoing risk assessment specific to the organization's business; policies and procedures to manage these risks; regular testing and monitoring of procedures; continuous efforts to address promptly any gaps or weaknesses; and communication policies to provide timely information to senior decision-makers, customers, other market participants, and regulators, as appropriate.

---

[1] See **OCIE Safeguarding Customer Records and Information in Network Storage—Use of Third Party Security Features** (May 23, 2019); **Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P— Privacy Notices and Safeguard Policies** (Apr. 16, 2019); **Observations from Investment Adviser Examinations Relating to Electronic Messaging** (Dec. 14, 2018); **Observations from Cybersecurity Examinations** (Aug. 7, 2017); **Cybersecurity: Ransomware Alert** (May 17, 2017); **OCIE's 2015 Cybersecurity Examination Initiative** (Sept. 15, 2015); **Cybersecurity Examination Sweep Summary** (Feb. 3, 2015); and **Investment Adviser Use of Social Media** (Jan. 4, 2012).

Access Rights and Controls

OCIE noted that organizations should consider a number of factors related to access rights, including ongoing review of the appropriate level of access of each user and whether the user's needs have changed. They also discussed methods to manage access, such as multi-factor authentication (MFA), and efforts to monitor actual access patterns. OCIE's reference to specific controls, such as MFA, is noteworthy because it signals that they may question whether firms have adopted such controls and ask for explanations if they have not. They also emphasized the importance of having more than just good policies and procedures; OCIE expects firms to test and monitor those controls frequently.

Data Loss Prevention

OCIE discussed a number of methods that organizations use to prevent data from being misappropriated or misused. These include vulnerability scanning; perimeter security to control, monitor, and inspect all incoming and outgoing network traffic; detective security to detect threats on endpoints; patch management; maintaining an inventory of hardware and software assets; utilizing encryption and network segmentation to secure data and systems; monitoring insider threats; and securing legacy systems and equipment. Patch management is particularly noteworthy because many widespread cyberattacks have taken advantage of vulnerabilities for which patches became available but were not uniformly implemented.

Mobile Security

OCIE observed that mobile devices and applications may create additional and unique vulnerabilities for organizations, and outlined several measures to manage risk linked to mobile access. These include having policies and procedures for using mobile devices, implementing security measures such as MFA, and training. These measures deserve particular attention as financial institutions routinely provide employees, contractors, and customers with mobile access to sensitive data and systems.

Incident Response and Resiliency

OCIE observed that many incident response plans address a number of different scenarios, include measures to satisfy notification requirements, assign staff to execute specific areas of the plan, and allow for testing and periodic assessment of the plan (including the use of tabletop exercises). To address resiliency, OCIE noted that organizations maintain an inventory of core business operations and systems, assess risks and prioritize business operations, and consider additional safeguards (such as backing up data on a different network or offline) in preparation for potentially disruptive cyber incidents. Our own observations are that maintaining an up-to-date inventory of sensitive data and essential systems, including their location on networks, can be particularly useful.

Vendor Management

OCIE noted that organizations with good vendor management programs ensure vendors meet security requirements; understand contract terms outlining the parties' rights, responsibilities, and expectations; and monitor and test vendors' cybersecurity measures. These points are an important reminder to regulated entities that OCIE expects them to engage with their vendors on cybersecurity. They also are a helpful message to vendors in the financial services industry about what their customers may come to expect.

Training and Awareness

OCIE noted that training and awareness are key to cybersecurity programs, and encouraged organizations to include examples and exercises in training and to monitor training effectiveness amongst employees. Once again, they noted specific practices, such as training employees to identify and respond to indicators of breaches and to obtain customer confirmation if behavior appears suspicious.

OCIE's observations are conveyed as a recitation of practices that they have encountered in exams. But the context and content communicate a fairly clear message: OCIE is giving guidance to the industry on cybersecurity practices that they believe are both important and at least somewhat common, and examiners may begin to press more aggressively on firms that, despite these observations, do not have similar controls in place.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres	212 450 4724	**greg.andres@davispolk.com**
Robert A. Cohen*	202 962 7047	**robert.cohen@davispolk.com**
Neil H. MacBride	202 962 7030	**neil.macbride@davispolk.com**
Annette L. Nazareth	202 962 7075	**annette.nazareth@davispolk.com**
Margaret E. Tahyar	212 450 4379	**margaret.tahyar@davispolk.com**
Leor Landa	212 450 6160	**leor.landa@davispolk.com**
Michael S. Hong	212 450 4048	**michael.hong@davispolk.com**
Matthew J. Bacal	212 450 4790	**matthew.bacal@davispolk.com**
Daniel F. Forester	212 450 3072	**daniel.forester@davispolk.com**
Matthew A. Kelly	212 450 4903	**matthew.kelly@davispolk.com**

* Mr. Cohen is admitted to practice in New York and Maryland, and is practicing in DC under the supervision of partners of the firm.