KIRKLAND & ELLIS

Kirkland AIM

OCIE Issues Observations on Cybersecurity and Resiliency; Supreme Court Refuses to Hear FINRA Pay-to-Play Challenge

14 February 2020

OCIE Issues Observations on Cybersecurity and Resiliency

On January 27, 2020, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a statement setting forth OCIE examination observations on industry practices and approaches to managing and combating cybersecurity risk and maintaining and enhancing operational resiliency for SEC-registered investment advisers, broker-dealers and other registrants. These OCIE observations reflect the SEC's continued focus in recent years on cybersecurity for registered advisers, including private fund managers.[1]

OCIE's observations included the following:

- *Governance and Risk Management*. OCIE noted that effective cybersecurity programs typically include a risk assessment, written policies and procedures to address identified risks and effective implementation and enforcement of those policies. OCIE further highlighted that certain organizations utilized certain practices, including: having senior leadership devote attention to cybersecurity and resiliency programs; establishing comprehensive testing and monitoring of cybersecurity practices; frequent updating to policies and procedures to address identified weaknesses; and establishing communication policies to provide timely information to clients or investors, employees, regulators and others as appropriate.
- *Access Rights and Controls*. OCIE noted that it had observed organizations that performed the following actions related to setting access rights and controls: determining a clear understanding of user information access needs; developing

processes that limit/terminate user access as appropriate; implementing separation of duties for user access approvals; re-certifying access rights on a periodic basis; requiring strong passwords and using multi-factor authentication systems; monitoring user access and developing procedures that monitor failed login attempts and requests for password changes and unusual customer requests; and developing procedures that require review and evaluation of changes to the systems.

- *Data Loss Prevention*. OCIE noted that it had observed the following measures that seek to ensure that sensitive data is not lost, misused or accessed by unauthorized users: routine scans of software and IT systems both within the organization and at applicable third party vendors; implementation of systems to control and monitor network traffic (e.g., firewalls, web proxy systems, intrusion detections systems, email security systems, blocking access to personal email, cloud-based file-sharing systems, social media and storage media such as CDs and USB drives); acquisition of products that can identify incoming fraudulent communications and enabling security features in software; establishment of a software patch management program; maintenance of an inventory of hardware and software assets; utilization of data encryption and access control techniques; creation of an "insider threat" program, including developing rules to block transmission of sensitive data out of the organization, conducting penetration tests and tracking corrective actions; and verification that disposed-of hardware and software does not create risks by removing sensitive information before disposal and reassessing risk as legacy systems are replaced.
- *Mobile Security*. OCIE noted that mobile devices and applications may create unique vulnerabilities and that it had observed organizations using the following mobile security measures, among others: specific policies for the use of mobile devices; using a mobile device management application for the business that works with all relevant devices (including "bring your own" devices, if applicable); use of multifactor authorization; bars on printing or moving information to personally owned electronic devices; acquisition of remote data clear functionality for devices that are lost or otherwise not within the organization's coverage; and employee training specifically related to mobile devices.
- *Incident Response*. OCIE highlighted that many organizations with incident response plans included the following elements: an approach that planned for various scenarios including denial of service attacks, malicious disinformation, ransomware, employee succession and more extreme but plausible scenarios; procedures that addressed, among other items, timely notification and response, escalation of matters to appropriate levels of management (including legal and compliance), and communication with key stakeholders; addressing legal reporting requirements (e.g., vis-à-vis law enforcement authorities, regulators, clients or investors, and

employees); assignment of roles in the event of an incident; and a practice of testing the plan and assessing the response.

- *Resiliency*. OCIE noted certain strategies to address operational resiliency (which OCIE noted is an important part of an incident response plan): a practice of identifying core business systems and identifying the impact of an individual system or process failure on the enterprise's other systems and business services as a whole; a determination of acceptable risk tolerances, taking into consideration potential substitutes during disruption, geographic separation of backup data, concentration risk and the consequences of business disruptions on the organization's stakeholders and other parties; and consideration of whether backup data should be on a different network and/or offline and whether cybersecurity insurance is appropriate.
- *Vendor Management*. OCIE noted that it had observed organizations use the following practices in connection with managing its vendor relationships: establishing a program to ensure that vendors met security requirements; using questionnaires based on reviews of industry standards as well as independent audits; establishing procedures to terminate or replace vendors; making sure that all terms in vendor contracts are clearly understood; understanding the risks associated with vendor outsourcing, including vendor use of cloud-based services; and monitoring of the vendor relationship (including continued compliance with security requirements and changes to vendor services or personnel).
- *Training and Awareness*. OCIE observed that when training staff about cybersecurity issues, many would: train staff to implement the organization's policies and procedures and build a culture of readiness and resiliency; provide specific examples and exercises to consider (e.g., phishing exercises and specific measures in connection with identifying and responding to signs of breach and obtaining customer confirmation of suspicious behavior); and continuously monitor attendance and the effectiveness of training.

OCIE further encouraged organizations to review the SEC's Cybersecurity Spotlight webpage and to sign up for alerts from the Department of Homeland Security's Cyber Infrastructure Security Agency.[2]

OCIE also reiterated that cybersecurity issues are a key priority, noting, among other things, that it has been a key element in its examination program for the past eight years and that it has published eight risk alerts related to cybersecurity.[3] In light of the SEC's continued focus on cybersecurity, registered advisers are encouraged to consider their existing policies and procedures in light of OCIE's observations and the industry practices named in the statement.

Supreme Court Refuses to Hear FINRA Pay-to-Play Challenge

On January 13, 2020, the Supreme Court denied the petition to hear an appeal of *New York Republican State Committee v. Securities and Exchange Commission*, which involved the New York Republican Party's challenge to FINRA Rule 2030, which imposes pay-to-play restrictions on the political contributions of broker-dealers and which largely mirrors the restrictions set forth in Advisers Act Rule 206(4)-5. The Supreme Court's denial leaves in place the D.C. Circuit's decision, which had rejected the New York Republican Party's challenge.

---

1. *See* OCIE Risk Alert Relating to Safeguarding Customer Records and Information in Cloud-Based and Other Network Storage, *Kirkland AIM* (May 30, 2019); OCIE Risk Alert Relating to Electronic Messaging, *Kirkland AIM* (Dec. 20, 2018); SEC Settles with Investment Adviser over Cybersecurity Procedures, *Kirkland AIM* (Oct. 1, 2018); SEC's OCIE Issues Cybersecurity Alert (May 18, 2017); Adviser Settles SEC Proceeding for Failure to Safeguard Customer Data, *Kirkland AIM* (June 23, 2016); SEC Brings Cybersecurity Enforcement Action Against Registered Adviser, *Kirkland AIM* (Sept. 24, 2015); and SEC's 2015 Cybersecurity Examination Initiative for Investment Advisers, *Kirkland AIM* (Sept. 21, 2015).↩

2. Other helpful resources highlighted by OCIE include industry association information-sharing groups such as the Financial Services Sharing and Analysis Center and the National Institute of Standards and Technology Cybersecurity Framework.↩

3. *See* 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).↩

Authors

Norm Champ, P.C.

Partner / New York

Scott A. Moehrke, P.C.

Partner / Chicago

Kevin R. Bettsteller

Partner / San Francisco

Michael Chu

Partner / Chicago

Matthew Cohen

Partner / San Francisco / Los Angeles – Century City

Marian Fowler

Partner / Washington, D.C.

Phil Vincent Giglio

Partner / Chicago

Nicholas A. Hemmingsen

Partner / Chicago

Alpa Patel

Partner / Chicago

Jaime Doninger Schechter

Partner / New York

Aaron J. Schlaphoff, P.C.

Partner / New York

Christopher J. Scully

Partner / Chicago

Robert H. Sutton

Partner / New York

Ryan P. Swan

Partner / Chicago

Jamie Lynn Walter, P.C.

Partner / Washington, D.C.

Josh Westerholm, P.C.

Partner / Chicago

Sunil Shenoi

Partner / Chicago

Related Services

Practices

- Investment Funds
- Transactional
- Data Security & Privacy
- Intellectual Property

accounting, or other professional advice or opinions on specific facts or matters and, accordingly, assume no liability whatsoever in connection with its use. Pursuant to applicable rules of professional conduct, portions of this publication may constitute Attorney Advertising.