The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 32179

January 28, 2020

OCIE Publishes Its Cybersecurity and Resiliency Observations

[32179]

January 28, 2020 TO: Chief Compliance Officer Committee
Chief Information Security Officer Advisory Committee
Technology Committee
Transfer Agent Advisory Committee SUBJECTS: Compliance
Cybersecurity RE: OCIE Publishes Its Cybersecurity and Resiliency Observations

OCIE has published a new document, *Cybersecurity and Resiliency Observations* ("*Observations"*), to share OCIE's insights relating to cyber security and resilience.[1] A key focus of OCIE's examination program over the past eight years has been information security and the insights in the *Observations* are from OCIE's exams conducted during this period. The document supplements the eight risk alerts OCIE has published during the past eight years related to cybersecurity. Its current publication groups OCIE's observations under the following headings:

- Governance and Risk Management
- Access Rights and Controls
- Data Loss Prevention
- Mobile Security
- Incident Response and Resiliency
- Vendor Management and
- Training and Awareness

The *Observations'* discussion of each of these issues is briefly summarized below. In addition to providing OCIE's observations on each of these topics, the *Observations* also lists some resources that registrants may want to utilize to stay informed of cyber threats and issues. These are also mentioned in this memo.

Governance and Risk Management

According to the *Observations,* effective cybersecurity programs begin with the right toNe at the top. OCIE has observed that key elements of effective governance include, among other things: (i) a risk assessment to identify, analyze, and prioritize cybersecurity risks to the organization; (ii) written cybersecurity policies and procedures to address those risks; and (iii) the effective implementation and enforcement of those policies and procedures. OCIE has observed firms using the following risk management and governance measures:

- Senior level engagement on the firm's cybersecurity and resilience programs;
- Establishing a risk assessment process to identify, manage, and mitigate those cyber risks that are relevant to the registrant's business, including identifying and prioritizing potential vulnerabilities (*e.g.,* remote or traveling employees, insider threats, international operations, geopolitical risks, etc.);
- Adopting written policies and procedures relating to cyber risks;
- Testing and monitoring to validate the cyber policies and procedures on a regular and frequent basis and in response to new threat information;
- Continuously evaluating the effectiveness of the firm's cyber program and addressing any gaps or weaknesses; and
- Establishing internal and external communications policies and procedures to provide timely information to decision makers, customers, employees, other market participants, and regulators, as appropriate.

Access Rights and Controls

According to the *Observations,* effective access controls include: (i) understanding the location of data, including client information, throughout an organization; (ii) restricting access to systems and data to authorized users; and (iii) establishing appropriate controls to prevent and monitor for unauthorized access. OCIE has observed firms addressing access rights and controls by: understanding who needs access to what information; limiting access based upon the user's need for access; conducting periodic access reviews; implementing separation of duties for user access approvals; re-certifying access rights on a periodic basis; requiring the use of strong passwords; periodically changing passwords; utilizing multi-factor authentication; and revoking system access when appropriate. Firms should also consider monitoring user access to systems on an ongoing basis and: monitor for failed login attempts and account lockouts; ensure proper handling of customers' requests for user name and password changes; procedures to authenticate anomalous or unusual customer requests; and investigating any anomalies.

Data Loss Prevention

Data loss prevention involves ensuring that sensitive data, including client information, is not lost, misused, or accessed by unauthorized users. In connection with data loss prevention, OCIE has observed firms engaging in:

- Vulnerability scanning;
- Controlling, monitoring, and inspecting all incoming and outgoing network traffic to prevent unauthorized or harmful traffic;
- Implementing the ability to detect threats on endpoints;
- Establishing a patch management program covering all software;
- Maintaining a current inventory of hardware and software assets;
- Encrypting data in motion or at rest on all systems and devices;
- Implementing network segmentation and access controls to limit data availability to only authorized systems and networks;
- Creating an insider threat program to identify suspicious behaviors; and
- Securing legacy systems and equipment when they are decommissioned or disposed of.

Mobile Security

To the extent firms use mobile devices or applications, they should consider: having policies and procedures governing the use of such devices; establishing a mobile device management strategy; implementing multi-factor authentication for all internal and external users; taking steps to prevent printing, copying, pasting, or saving information to

personal devices; ensuring the ability to remotely delete data from a device; and training employees on mobile device security.

Incident Response and Resiliency

Incident response involves: (i) the timely detection and reporting of cyber incidents; and (ii) assessing the appropriateness of corrective actions taken in response to such incidents. As part of effective incident response and resilience, OCIE has observed registrants:

- Developing a comprehensive risk-based incident response plan for a variety of cyber events;
- Complying with applicable federal or state reporting requirements applicable to cyber events;
- Designating employees with specific roles and responsibilities in the event of a cyber incident; and
- Testing and assessing the incident response plan on an ongoing basis.

With respect to strategies to address resiliency, OCIE has observed firms: (1) maintaining an inventory of core business operations and systems; (2) understanding core services and vulnerabilities, including services that the firm does not directly control; (3) understanding system redundancies or backups; (4) avoiding concentration risks; and (5) considering the effects of business disruptions on both the firm's stakeholders and other organizations.

Vendor Management

OCIE has also observed firms considering cyber as part of their vendor management. These considerations include, for example, whether vendors are able to meet security requirements and safeguard information; whether contractual terms adequately address rights, responsibilities, and expectations; understanding risks associated with vendors' use of cloud-based services; ensuring that, overtime, a vendor continues to meet security requirements; and monitoring the vendor to be aware of changes to the vendor's services or personnel.

Training and Awareness

According to OCIE, training and awareness are key components of cybersecurity programs. OCIE has observed the following practices used by firms as part of their cybersecurity training and awareness: training staff to implement the firm's cybersecurity policies and procedures; engaging the workforce to build a culture of cybersecurity readiness and operational resiliency; providing specific cybersecurity and resiliency training; including preventive measures in training; monitoring attendance at training; assessing the effectiveness of the training program; and continuously updating training programs based on cyber threat intelligence.

Additional Resources

The *Observations* note OCIE's commitment to work with federal and local partners, market participants, and others to monitor developments and effectively respond to cyber threats. OCIE offers the following as resources to firms:

- The SEC's Cybersecurity Spotlight page (www.sec.gov/spotlight/cybersecurity);
- Signing up to receive alerts from the Cyber Infrastructure Security Agency (CISA),[2] which is the part of the U.S. Department of Homeland Security that is responsible for protecting the nation's critical infrastructure from physical and cyber threats; and
- Participating in the Financial Services Information Sharing and Analysis Center (FS-ISAC, www.fsisac.com), which provides a mechanism for collaborating across industry

and governing on cyber issues.

Another resource mentioned in the *Observations* is the National Institute of Standards and Technology Cybersecurity Framework (https://www.nist.gov/cyberframework), which provides a mapping of cybersecurity control objectives to industry standards, guidelines, and practices designed to promote the protection of critical infrastructure.

◆ ◆ ◆

The *Observations* conclude by encouraging market participants to both review their practices, policies and procedures relating to cyber and operational resiliency and actively engage with regulators and law enforcement in this effort. It additionally notes that OCIE will continue to focus on working with firms to identify and address cyber security risks.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] OCIE's *Observations* are available at: https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

[2] The *Observations* provide the following link that can be used to sign up for CISA alerts: https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new.