Debevoise & Plimpton

Debevoise In Depth

SEC's New Cyber Observations Highlight Operational Resiliency

February 4, 2020

New cybersecurity advice from the U.S. Securities and Exchange Commission ("SEC") examination staff highlights the importance of operational resiliency, mobile security, a cross-functional approach to cyber risk management, and the sharing of threat intelligence across corporate boundaries.

The guidance takes the form of a January 27, 2020 publication from the SEC's Office of Compliance Inspections and Examinations ("OCIE").[1] OCIE's "Cybersecurity and Resiliency Observations" are based on thousands of examinations of the investment advisers, broker-dealers, and similar firms over which the SEC has inspection authority. The SEC also has ramped up its focus on cybersecurity for corporate America more generally—advising that a substantively robust cybersecurity program is necessary to help public companies meet their disclosure obligations under the securities laws. [2] The new report thus demands attention from both registrants that OCIE directly oversees and across the public and private sectors more broadly.

What's New?

- **Emphasis on Resiliency**. OCIE mentions "operational resiliency" in the title of its risk alert and repeatedly in the text. This is in keeping with increased focus on business continuity management from other regulators,[3] and represents a notable expansion of OCIE's focus. Its prior cyber risk alerts were silent as to operational resiliency concerns.

[1] U.S. Securities and Exchange Commission, *Cybersecurity and Resiliency Observations: Office of Compliance Inspections and Examinations* (Jan. 27, 2020), available here (pdf).

[2] U.S. Securities and Exchange Commission, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures,* available here (pdf).

[3] The Federal Financial Institutions Examination Council (FFIEC) updated its Business Continuity Management handbook in November 2019; the updated handbook is available here (pdf).

- **Mobile Security**. OCIE also elevated its discussion of mobile device and application security, an area that garnered just one mention in its 2017 observations.[4] Regulated entities should evaluate their relevant policies, procedures, and standards, and expect questions related to mobile security in their next OCIE exam.

- **Cross-Functional Approach**. OCIE underscores that cybersecurity risk management and incident response should touch every part of the organization, not solely the Information Technology function. Firms should consider how non-technical groups, such as Communications and Legal, can be an effective part of the firm's cybersecurity risk mitigation.

- **Information Sharing**. For the first time, OCIE encourages regulated entities to sign up for alerts through the Cyber Infrastructure Security Agency ("CISA") or join information sharing groups, such as the Financial Services Information Sharing and Analysis Center ("FS-ISAC").

Summary of Examination Observations

OCIE staff identified a number of practices that regulated entities should consider when implementing and maintaining their cybersecurity programs. Unlike in the 2017 observations, OCIE did not identify systemic issues or inadequate practices it had identified during examinations, but instead focused on describing the elements of effective cybersecurity and resiliency programs the staff has observed during examinations.

Recognizing that there is no such thing as a "one-size fits all" cybersecurity program, OCIE identifies seven focus areas: (1) Governance and Risk Management; (2) Access Rights and Controls; (3) Data Loss Prevention; (4) Mobile Security; (5) Incident Response and Resiliency; (6) Vendor Management; and (7) Training and Awareness.

Governance and Risk Management

- **Tone at the Top**. Devote board and senior leadership attention to establishing and overseeing the firm's cybersecurity and resiliency program.

- **Risk Assessment**. Develop and implement a risk assessment process that contemplates the organization's business model and considers a broad range of technical and non-technical threats and vulnerabilities.

[4] U.S. Securities and Exchange Commission Office of Compliance Inspections and Examinations, *Observations from Cybersecurity Examinations* (Aug. 7, 2017), available here (pdf).

- **Implement and Test Policies and Procedures**. Adopt comprehensive written policies and procedures that are periodically updated and reviewed by the board or senior leadership as appropriate. Establish comprehensive and frequent testing and monitoring to validate.

- **Communications**. Establish communications policies and procedures to timely engage internal and external stakeholders.

Access Rights and Controls

- **Understand User Access**. Develop a clear understanding of access needs to systems and data, and ensure that access rights are tailored to needs. Perform periodic reviews to ensure access rights are up to date.

- **Access Management**. Manage user access by employing systems or procedures that:

  - implement role-based restrictions on access at all phases of employment;
  - employ separation of duties for user access approvals;
  - audit user access rights on a periodic basis;
  - require the use of strong, periodically changed passwords;
  - utilize multi-factor authentication; and
  - revoke access immediately upon termination.

- **Access Monitoring**. Maintain processes and procedures to monitor for unauthorized use of employee and customer credentials and investigate anomalies. Continuously review in light of hardware and software changes.

Data Loss Prevention

- **Scanning**. Establish and maintain a comprehensive vulnerability and patch management program, with routine scanning.

- **Perimeter Security**. Implement capabilities to control, monitor, and inspect inbound and outbound network traffic and detect unauthorized or harmful traffic, and have an enterprise-wide data loss prevention solution to block access to personal email, file sharing, and social media.

- **Endpoint Threat Detection**. Leverage tools to detect threats on endpoints, such as firm-issued devices, including products that use signature and behavioral capabilities to identify incoming fraudulent communications.

- **Inventory**. Maintain a hardware and software inventory, including "crown jewel" assets and information. Verify that systems that are no longer in use do not pose a security threat to the firm. Secure legacy systems and equipment.

- **Encrypt and Segment**. Encrypt data "in motion" and "at rest." Implement network segmentation and access controls to limit unauthorized access.

- **Monitor Insiders**. Create an insider threat program to identify and address suspicious behaviors. Test systems and create rules to block transmission of sensitive data.

Mobile Security

- **Policies and Procedures**. Establish policies and procedures for both firm-issued and employee-owned devices.

- **Device Management**. Leverage a mobile device management application or similar technology to control access to firm communications and data.

- **Security Measures**. Implement key security measures, including multi-factor authentication for all remote users, limitations on transferring data between personal and firm-issued devices, and the ability to remotely delete content and data from a lost or stolen device.

- **Training**. Train employees on mobile device policies and effective practices to protect mobile devices.

Incident Response and Resiliency

- **Develop an IRP**. Develop a risk-assessed incident response plan, in light of past events and current threat intelligence, that:

    - establishes processes for timely notification to internal and external stakeholders;

    - defines procedures for escalating an incident to senior management;

    - designates roles and responsibilities in the event of a cyber incident;

   - addresses applicable reporting requirements to consumers, regulators, and other interested parties; and

   - includes provisions to ensure business continuity and resiliency.

- **Have an Operational Resiliency Strategy**. Maintain an inventory of core business operations and systems. Develop an operational resiliency strategy that prioritizes business continuity, avoids concentration risk, and considers business disruptions to internal and external stakeholders.

- **Continuous Testing and Improvement**. Test the firm's incident response plan and potential recovery times on a periodic basis. After an incident, assess the response and update the IRP as appropriate.

Vendor Management

- **Have a Program**. Establish a vendor management program to ensure vendors meet security requirements and implement appropriate safeguards.

- **Understand Relationships**. Ensure that contract terms establish the appropriate rights, responsibilities, and expectations regarding cybersecurity risk and standards.

- **Monitor and Test**. Continually monitor the vendor relationship to ensure compliance and up-to-date awareness of services and personnel.

Training & Awareness

- **Use Training to Build Culture**. Train staff to implement the firm's cybersecurity policies and procedures. Foster a culture of cybersecurity readiness and operational resiliency.

- **Use Realistic Exercises**. Provide specific cybersecurity and resiliency training, such as phishing exercises and training on identifying and responding to early indicators of incidents.

- **Monitor Effectiveness**. Ensure that employee training is effective, and update trainings based upon new threat intelligence.

* * *

As always, we are available to discuss these issues with our clients and friends. Please do not hesitate to contact us with any questions.

New York

Jeremy Feigelson
jfeigelson@debevoise.com

Avi Gesser
agesser@debevoise.com

Jim Pastore
jjpastore@debevoise.com

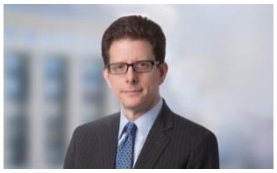
Lisa Zornberg
lzornberg@debevoise.com

Stephanie M. Cipolla
smcipolla@debevoise.com

Christopher S. Ford
csford@debevoise.com

Washington, D.C.

Luke Dembosky
ldembosky@debevoise.com



Robert B. Kaplan
rbkaplan@debevoise.com

Julie M. Riewe
jriewe@debevoise.com

H Jacqueline Brehmer
hjbrehmer@debevoise.com