PUBLICATION

SEC Dispatches on Cybersecurity

Authors: Alisa L. Chestler
February 10, 2020

2020 OCIE Priorities

On January 7, 2020, the Securities Exchange Commission's (SEC) Office of Compliance Inspections and Examination (OCIE) released its "2020 Examination Priorities," which included a focus on information security programs. The OCIE plans to continue to focus on information security for each of its existing five examination programs. Ultimately, OCIE's goal is to assist with and enforce the implementation of proper safeguards of cybersecurity to protect registrants and other market participants.

2019 was a record year for incidents involving ransomware, business email compromises, theft of intellectual property and other cyber incidents that had significant and sometimes devastating effects on companies of all sizes. In an effort to ensure companies remain vigilant, the OCIE released the "Cybersecurity and Resiliency Observations" designed to inform companies and help them prepare for audits by the OCIE. All regulated entities should pay careful attention to the lessons and ensure documentation designed to meet SEC expectations. OCIE examines the following areas of cybersecurity: (i) governance and risk management; (ii) access rights and controls; (iii) data loss prevention; (iv) mobile security; (v) incident response and resiliency; (vi) vendor management; and (vii) training and awareness.

Governance and Risk Management

Culture and leadership are key to a mature program. OCIE expects leadership in regulated companies to ensure a commitment to an effective cyber program. OCIE will review and ask questions regarding the governing culture of an organization. Programs vary on a case-by-case basis, but OCIE stated that the most successful governance has the following: (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 also observed organizations that have implemented top-down approaches from senior management and the board provided successful roadmaps for tackling cybersecurity issues within an organization.

Access Rights and Controls

Good information systems controls include proper user rights and access. OCIE identifies the following access controls that organizations should adopt: (i) understanding location of data throughout the organization; (ii) restricting access to the location of data to authorized users; and (iii) establish appropriate controls to prevent and control for unauthorized access. All of these actions should be coupled with effective access management and monitoring of an organization's data and transfer of such data.

Data Loss Prevention

Technical systems and monitors are necessary to protect information. In order to prevent the loss of data at an organization, OCIE has suggested the following measures: (i) vulnerability scanning; (ii) perimeter security; (iii) detective security; (iv) patch management; (v) inventory hardware and software; (vi) encryption and network segmentation; (vii) insider threat monitoring; and (viii) securing legacy systems and equipment. Systems and threats are always changing, thus requiring the need for constant reevaluation of current practices and cyber landscapes.

Mobile Security

OCIE has noted that the use of mobile devices, which is ubiquitous throughout industry, creates different cybersecurity challenges for organizations. It has noted the following practices should be utilized to manage mobile applications: (i) sufficient policies and procedures for mobile devices; (ii) management of the use of mobile devices, including a mobile device management application; (iii) implementing security measures; and (iv) the training of employees.

Incident Response and Resiliency

Even the most sophisticated and mature companies can suffer a cyber incident. A good incident response program can prevent a minor incident from becoming a catastrophic event. To develop an incident response plan, companies should (i) identify applicable reporting requirements to state and local authorities; (ii) have the response team and their responsibilities articulated; and (iii) testing of the plan. Organizations need to consistently test the resilience of these response plans. Without the testing of scenarios, the core business services and the risk tolerance of an organization cannot be completely understood.

Vendor Management

Vendors can represent one of the largest risks to a company. OCIE recommends the following procedures: (i) due diligence for vendor selection; (ii) monitor the vendors and their contract terms; (iii) assess vendor relations to monitor the risk assessment process; and (iv) monitor how vendors protect their client information. Ultimately, a common manner to assess these items is to a create a vendor management program to monitor and ensure vendors follow a specific policy.

Training and Awareness

Employees must be trained on cybersecurity awareness. The following training procedures are exhibited across many organizations: (i) policies and procedures as a training guide; (ii) include examples and exercises in training; and (iii) measure training effectiveness.