Cybersecurity: Key Considerations Developed by OCIE

The SEC's Office of Compliance Inspections and Examinations published a series of observations gleaned from thousands of exams over a period of years. While OCIE's charge is the inspection of certain SEC registrants the observations of the exam staff offer important lessons for all in this critical and constantly evolving area. The observations are set-forth in Cybersecurity and Resiliency Observations, Office of Compliance Inspections and Examinations (Jan. 27, 2020) (here), detailed below.

Related Capabilities

- Securities & Financial Services Litigation & Enforcement
- Privacy & Social Media

Governance and risk management

An effective cybersecurity program begins with "tone at the top" and the involvement of senior enterprise executives. Several key building blocks are essential: Ongoing tailored risk assessments and testing; adopting and promptly adapting cybersecurity policies and procedures to address risks; and communication with clients, employees and regulators in a timely manner.

Access rights and controls

The central issue is understanding where data is located throughout an enterprise, and what the access needs are to that data. The identification of the appropriate users permits delimiting access, whereas establishing controls allows a firm to prevent and monitor for unauthorized access. Three key elements should be prioritized: Access which is based on, and limited by, need; policies governing access management, especially during onboarding, transfer and terminations; and monitoring user access for adherence to the policies and procedures.

Data loss prevention

This typically includes tools used to ensure that sensitive data and client information is not lost or misused. Key measures include: Vulnerability scanning of software code, servers, databases and other applications; perimeter security to control, monitor and prevent unauthorized network traffic; detective security which identifies threats on

endpoints; patch management covering all software and hardware; maintaining an inventory of hardware and software and how they are protected; encryption and network segmentation through the use of tools and processes designed to secure data and systems; insider threat monitoring for suspicious behaviors; and securing legacy systems and equipment so that disposal does not create vulnerabilities.

Mobile security

Mobile devices can create additional, and unique, concerns regarding security. Effectively dealing with these issues requires: Policies and procedures designed specifically for mobile devices; and the use of mobile device management technology. If personal devices are used, the program must be designed to cover all such devices. In addition, precautions must be taken to prevent the duplication or saving of sensitive or proprietary information on personal devices, with all of these policies and practices being the subject of specific employee training.

Incident response and resiliency

Two points to be considered are: First, the organization should have a plan with component elements that include: Developing risk assessment for various scenarios such as service attacks, malicious disinformation, ransomware, and others. Second, the applicable federal and state reporting requirements must be addressed. Third, strategies focused on resilience are required that include: Maintaining an inventory of core business operations and systems; and assessing risk tolerances tailored to the organization and maintaining the necessary back-up data.

Vendor management

Vendor management requires a program that includes: Elements to ensure that vendors, upon selection and thereafter, protect client information and implement appropriate safeguards; understating the contractual terms, relating to risks and security, that govern the relationship; appropriate monitoring and testing, leveraging independent internal control testing such as SOC 2 and SSAE 18; and establishing procedures for terminating or replacing vendors.

Training and awareness

Key to any strong cybersecurity program is the training and awareness of employees. OCIE observed policies and procedures being used as a training guide for staff to foster cybersecurity readiness and operational resiliency, emphasizing the importance of engaging employees through various exercises. The program should also periodically evaluate its effectiveness.

In the end, cybersecurity is a multi-faceted challenge which requires a compliance program tailored to the business of each organization. A strong program begins with the tone at the top that flows through the enterprise and is focused on both the evolving cyber-threats and related risks faced by the particular business and its clients.