7 Key Takeaways from SEC Observations on Industry Cybersecurity and Resiliency Practices

February 12, 2020

The Securities and Exchange Commission's ("SEC") Office of Compliance Inspections and Examinations ("OCIE") recently issued examination observations ("Release") connected to cybersecurity and related operational resiliency practices. The observations stem from OCIE's examinations of thousands of SEC registrants, including broker-dealers, investment advisors, clearing agencies, and national securities exchanges. In recent years the SEC has increased its focus on cybersecurity risk management, with particular attention to market systems, customer data protection, and disclosure of material cybersecurity risks and incidents.

This comprehensive Release reinforces the SEC's commitment and highlights cybersecurity as an essential component of an organization's compliance program.

Following are some highlights of the observations OCIE shared in the Release:

Governance and Risk Management

Effective cybersecurity programs begin with committed senior leaders who are engaged in the process by working with staff to understand, prioritize, communicate, and mitigate cybersecurity risks. OCIE also discussed the benefits of incorporating a governance and risk management process into cybersecurity programs that generally includes:

- a risk assessment to identify, analyze, and prioritize cybersecurity risks to the organization;
- written cybersecurity policies and procedures to address those risks; and
- the effective implementation and enforcement of those policies and procedures. Central to these recommendations is the ongoing evaluation of their efficacy.

Access Rights and Controls

OCIE identified processes and procedures organizations use to establish appropriate levels and types of user access. There should be a clear understanding of the location of data (especially client data), and access needs to systems and data. User access to sensitive systems and data should be limited based upon the need to perform legitimate and authorized activities. In addition to requiring the use of strong, and periodically changed passwords, effective access management includes multi-factor authentication, and immediately revoking system access for individuals who are no longer authorized. Appropriate access monitoring ensures that any access changes are approved and properly implemented and that any anomalies are investigated.

Data Loss Prevention

OCIE detailed several methods and tools organizations use to prevent the misappropriation or misuse of sensitive data. These include routine vulnerability scanning; perimeter security such as firewalls to monitor network traffic; detective security to detect threats on endpoints; patch management programs covering all software; maintaining an inventory of hardware and software assets; encrypting data and implementing network segmentation; creating an insider threat program to identify suspicious behaviors; and securing legacy systems and equipment by verifying that the decommissioning and disposal of hardware and software does not create system vulnerabilities.

Mobile Security

Mobile devices present added security vulnerabilities to organizations, in part because they may permit unintended access to sensitive data and systems. OCIE emphasized the importance of a mobile device management application or similar technology compatible with all mobile phone/device operating systems. OCIE also observed organizations requiring multi-factor authentication, taking steps to prevent printing, copying, pasting, or saving information to personally owned devices, and ensuring the ability to remotely clear data and content from a device owned by a former employee or a lost device.

Incident Response and Resiliency

Key components of incident response plans include business continuity and resiliency. Specifically, they address how quickly the organization can recover and safely serve clients following an incident. OCIE observed that many organizations with incident response plans generally had developed risk-assessed plans that included the following:

- compliance with applicable federal and state reporting requirements for cyber incidents or events;
- designated employees with specific roles and responsibilities in the event of a cyber incident;
- tested incident response plans and potential recovery times;
- identified and prioritized core business services and an understanding of the impact of an individual system or process failure on these services;
- assessed risks and prioritized business operations; and
- additional safeguards, such as maintaining back-up data in a different network and offline or obtaining cybersecurity insurance.

Vendor Management

OCIE’s observations with respect to vendor management suggest that conducting the appropriate level of due diligence is central to the effective management of third-party service providers. Some practices OCIE noted included organizations establishing a vendor management program to ensure vendors meet security requirements and implement appropriate safeguards. Firms must understand how risk and security are addressed contractually in terms of rights, responsibilities and expectations. They also conduct ongoing monitoring and testing to ensure the vendor continues to meet security requirements.

Training and Awareness

OCIE emphasized the importance of training and awareness in the maintenance of the cybersecurity program. Organizations used their policies and procedures to train staff and create a culture of cybersecurity readiness and operational resiliency. Effective training includes specific examples and exercises, as well as how to identify and respond to indicators of breaches. Organizations also should routinely re-evaluate and update their training programs based on cyber threat intelligence.

Conclusion

OCIE acknowledged that there is no “one-size-fits-all” approach to cybersecurity, and that the approaches highlighted in the Release may not be appropriate for all organizations. The observations are intended to serve as guidelines for firms considering how to improve their cybersecurity preparedness and response procedures. Contact Foreside to learn more about how we can help your organization develop, modify, or manage a comprehensive cybersecurity program.

Learn more about the Release here

Home