BRACEWELL

INSIGHTS

SEC Examiners Release Cyber Observations: What You Need To Know

February 5, 2020

On January 27, 2020, the SEC's Office of Compliance Inspections and Examinations (OCIE) ***announced*** its most recent Cybersecurity and Resiliency Observations. This report highlights specific practices that have been, and can be taken to enhance cybersecurity preparedness and incident response. The release of these observations is the latest move by the SEC demonstrating its increased attention to corporate cybersecurity practices. If you are a market participant supervised by OCIE, you may want to consider this report a benchmark to help navigate the SEC's expectations when reviewing internal cybersecurity programs. The SEC has indicated that cybersecurity compliance and procedures remain a top priority—and they should be for you too.

OCIE Cybersecurity and Resiliency Observations

The OCIE, which reviews the effectiveness of market participants' compliance programs, focused on seven areas in the cybersecurity report: governance and risk management; access rights and controls; data loss prevention; mobile security; incident response and resiliency; vendor management; and training and awareness. OCIE explained that it "felt it was critical to share these observations in order to allow organizations the opportunity to reflect on their own cyber-security practices."

OCIE made clear that the most effective cybersecurity programs were those with proactive senior leaders committed to improving their organization's cyber posture before an incident occurs. "Devoting appropriate board and senior leadership attention to setting strategy of and overseeing the organization's cybersecurity and resiliency programs," was a key observation.

Preventing data loss is a perennial focus of cybersecurity programs. OCIE observed a variety of tools and practices to ensure that sensitive data, including client information, was not lost, misused, or accessed by unauthorized users. These included frequent vulnerability scans of software and devices, utilizing encryption, keeping software patched with the latest updates, and monitoring for insider threats. On that last point, OCIE observed companies creating insider threat programs to identify specious behaviors, including escalating issues to senior leadership as appropriate.

Consistent with cybersecurity guidance from other sources but relatively new from the SEC, the report highlighted the risks associated with mobile devices, urging the implementation of security measures to prevent unauthorized access to sensitive systems. As corporate employees increasingly rely on mobile devices for work, the amount of sensitive data stored on those devices continues to grow, creating unique security concerns. OCIE observed companies

implementing security measures that prevent users from saving sensitive information to personally owned devices and maintaining the ability to remotely clear data on employees' devices, if necessary.

Addressing vendor management, OCIE underscored the increased risk related to vendor use of cloud services and the importance of due diligence when selecting vendors. Lastly, and arguably the most important topics addressed were incident response and training. OCIE stressed that market participants should be consistently testing and updating their incident response plans and training employees to identify and respond to cyber threats. These seven areas of focus provide important guidance for market participants regarding the expectations of OCIE examiners when conducting reviews.

Takeaways

With the release of the 2020 observations, the SEC continues to send the clear message that it expects market participants to not only respond timely and responsibly to cyber incidents, but also to proactively implement mitigation policies to reduce threats. Importantly, OCIE recognized that there is no one-size-fits-all approach.

Every organization should develop incident response plans that are tailored to their unique circumstances. Regulators continue to emphasize that is not enough to simply have policies on the books—companies must routinely update and practice those plans. Senior leaders should be involved in that process and should be prepared for the SEC and other regulators to closely examine their plans and other internal security protocols. Failure to do so is not only a regulatory issue, but creates private litigation risk.

The SEC is paying attention to and reiterating a common cybersecurity compliance roadmap: develop and implement cybersecurity plans to reduce risks, be prepared for regulatory scrutiny that may follow a cybersecurity incident, conduct staff training, and be prepared to respond to cybersecurity incidents.