CARLTON FIELDS

# OCIE Continues Relentless Cybersecurity Focus

April 13, 2020

The level of attention that the SEC's Office of Compliance Inspections and Examinations has been giving to cybersecurity issues can hardly be overstated.

For many years, OCIE has highlighted cybersecurity in its annual list of examination priorities, and the list for 2020, released on January 7, is no exception. Building on that, OCIE on January 27 released detailed examination observations regarding securities industry cybersecurity and operational resiliency practices. This follows no fewer than eight cybersecurity risk alerts issued by OCIE within the past eight years.

The examination observations summarize cybersecurity risk management practices observed by OCIE during thousands of examinations and are offered "to assist market participants in their consideration of how to enhance cybersecurity preparedness and operational resiliency."

The observations are organized under seven broad headings and highlight many practices and procedures that most firms, in our experience, probably already have in place. This includes basics like performing risk assessments; having written cybersecurity policies and procedures; properly using encryption, network segmentation, and access controls; training employees; and having, practicing, and reassessing incident response plans.

The examination observations also highlight standard cybersecurity measures whose omission or missteps have been responsible for some of the most headline-grabbing breaches: detecting endpoint threats, having a patch management program, and properly managing vendor relationships and contracts. Ultimately, however, **the observations do not move the needle much on cybersecurity**. And although OCIE rightly points out the importance of certain measures, like controls to prevent and monitor for unauthorized access and "build[ing] a culture of cybersecurity readiness and operational resiliency," i**t has little to say about** the **"how" and "how much"** that are essential to almost any cybersecurity determination.

The examination observations do, however, offer **insight** into **what cybersecurity practices OCIE is likely to expect and ask about** during an examination and areas in which the SEC, or if breaches occur, private litigants, might allege deficiencies. Accordingly, firms should review their cybersecurity programs in light of the examination observations and consider documenting their reasons for variances.

## Authored By

Patricia M. Carreiro

## Related Practices

Cybersecurity and Privacy
Financial Services Regulatory

## Related Industries

Life, Annuity, and Retirement Solutions
Securities & Investment Companies