BCLP. Client Intelligent

BCLPSecCorpGov.com

SEC ALERTS PUBLIC COMPANIES OF INCREASE IN SOPHISTICATED RANSOMWARE ATTACKS

Jul 16, 2020

The SEC's Office of Compliance and Examinations (OCIE) issued a risk alert on July 10 about its observation of an apparent increase in sophistication of ransomware attacks on SEC registrants, including broker-dealers, investment advisers, investment companies, and impacting service providers to public financial institutions.

Recognizing the SEC's alert and other recent cyber incidents, we encourage all public companies, financial institutions and their service providers to consider their cybersecurity preparedness and operational resiliency to address hacking and, in particular ransomware attacks, consistent with the advice of the OCIE and the Department of Homeland Security. This is particularly important given that OCIE once again advised financial institutions, in its 2020 Examination Priorities release, that Information Security was one of its top priorities.

In its risk alert, OCIE cited recent reports of one or more threat actors orchestrating phishing and other campaigns designed to penetrate financial institution networks, primarily to access internal resources and deploy ransomware, a type of malware designed to provide unauthorized access to institutions' systems and deny the institution use of its system until a ransom is paid. OCIE also noted ransomware attacks impacting service providers to public companies.

OCIE encouraged public companies and their service providers to monitor cybersecurity alerts published by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), including the alert published on June 30, 2020, relating to a particular malware focused on financial institutions and their customers.

The OCIE alert noted that information security is a key risk area on which public companies and financial institutions should focus and that cybersecurity has been a key examination priority for OCIE for many years. OCIE also issued a special release earlier this year, entitled "Cybersecurity and Resiliency Observations."

Measures observed by the OCIE for public companies to consider in enhancing cybersecurity preparedness and operational resiliency were reported to include:

- Identifying systems and processes capable of being restored during a disruption, including ensuring geographic separation of back-up data and writing back-up data to an immutable storage system;
- Providing specific cybersecurity and resiliency training within organizations;
- Ensuring systems, software and anti-virus/anti-malware solutions are updated automatically and regularly;
- Managing user access through certification and authentication procedures; and
- Employing best practices for perimeter security capabilities to control and monitor network traffic.

In the event of a security breach, a public company or financial institution may, depending on the nature of the breach, have an obligation under federal and/or state law to notify impacted individuals. FINRA broker-dealers may, moreover, have an obligation to report such a breach to FINRA under Rule 4530(b).

Watch for continued SEC emphasis on cybersecurity disclosure issues, with particular attention to market systems, customer data protection, disclosure of material cybersecurity risks and incidents, and compliance with legal and regulatory obligations under the federal securities laws.

RELATED PRACTICE AREAS

- Securities & Corporate Governance

MEET THE TEAM

Jeffrey A. Ziesman

Kansas City

jeff.ziesman@bclplaw.com
+1 816 374 3225
