BCLP. Client Intelligent

Insights

SEC ENCOURAGES ENHANCED DATA SECURITY IN WAKE OF INCREASINGLY SOPHISTICATED RANSOMWARE ATTACKS FOLLOWING NAIC BRIEF ENCOURAGING ADOPTION OF DATA SECURITY MODEL LAW

Jul 17, 2020

The SEC's Office of Compliance and Examinations (OCIE) issued a risk alert on July 10th 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. Ransomware attacks are 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.

Insurance companies of all sizes and their technology and other service providers are equally vulnerable to these increasing attacks as recognized by the National Association of Insurance Commissioners (NAIC) promoting its Insurance Data Security Model Law, adopted in only 11 jurisdictions as of June 16, 2020 with legislative action considered in only 6 jurisdictions so far.

In its June 2020 State Legislative Brief, the NAIC noted that the U.S. Treasury Department has urged prompt action by states to adopt the Model Law within the next 5 years or the administration will ask Congress to take preemptive legislative action to set forth uniform requirements for insurer data security.

The SEC's July alert highlights this urgency by encouraging all financial services industry participants to implement robust monitors and protections against cyber crimes.

We encourage all SEC registrants, insurers and insurance industry market participants to consider their cybersecurity preparedness and operational resiliency that address hacking and, in particular ransomware attacks. Such consideration should be consistent with the advice of the OCIE, the Department of Homeland Security and state legislation adopting the NAIC Model Law applicable to insurance companies. This is particularly important given that the OCIE and state insurance regulators have advised that Information Security is a top priority.

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 encouraged registrants 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. State insurance regulators, even where the Model Law has not been adopted, similarly place a high priority on protecting consumer information through comprehensive data security policies and procedures.

The OCIE alert noted that information security is a key risk area on which registrants, and particularly financial institutions and their service providers, 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, public companies, insurers and other financial institutions may, depending on the nature of the breach, have an obligation under 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 NAIC and SEC emphasis on cybersecurity monitoring and protections, disclosure issues giving particular attention to market systems, customer data protection, disclosure of material cybersecurity risks and incidents, and compliance with legal and regulatory obligations under both state insurance laws and federal securities laws.

RELATED CAPABILITIES

- Securities & Corporate Governance
- Insurance & Reinsurance
