August 11, 2020

SEC Warns Industry: Remain Vigilant of Cyberattacks

Cybersecurity has been a key examination priority for the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) for many years. On July 10, 2020, it issued a risk alert warning of a surge in cyberattacks. The alert, which comes after a number of successful cyberattacks on market participants, reiterated OCIE's commitment to work with the industry, government authorities, and others to monitor cybersecurity developments, effectively respond to cyber threats, and work toward solutions that may help to prevent these attacks.

OCIE began by warning the industry that bad actors were using increasingly sophisticated tactics to compromise systems and deploy ransomware. Ransomware is a type of malware designed to gain unauthorized access to the systems of institutions and take the system and any confidential or sensitive information hostage until the institution agrees to pay compensation for its release. Additionally, OCIE warned that registrants (e.g., broker-dealers, investment advisors and investment companies) were not the only targets of such attacks, as ransomware attacks on the vendors and service providers utilized by registrants were increasing as well. Vendors and service providers make for attractive cyberattack targets, as these entities are generally responsible for storing and maintaining a wide range of sensitive information across a large and varied client base. Consequently, OCIE encouraged registrants to share information with their service providers, including information disclosed in the alerts issued by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency.

OCIE's reminder was timely, as news of a ransomware attack on a vendor of a large fund administrator became public a few weeks after the alert's release. The vendor, who developed and managed the administrator's investment dashboard and online enrollment portal, was infiltrated by bad actors who demanded the vendor pay a ransom for the release of files containing the sensitive data of a variety of the administrator's fund clients. The

vendor declined to pay the ransom and as a result, that data (which included names and email addresses) was released online.

In light of increasing threats, such as that experienced by the administrator's vendor, OCIE's alert also included a number of observations made through its examinations. While OCIE recognized that a diverse industry required varied solutions, OCIE suggested that a robust and comprehensive cybersecurity program should, among other things:

- Employ and maintain robust contingency and disaster recovery plans, including plans for how to respond and communicate with internal and external parties in a timely manner, including federal and state regulators and law enforcement.
- Identify systems and processes that are capable of being restored during a disruption so that business services can continue to be delivered, including ensuring a storage system exists in the event that primary data sources are compromised.
- Provide specific cybersecurity training, including phishing exercises to help employees identify phishing emails and better understand cyber risks and their responsibilities in helping to avert cyber threats such as ransomware.
- Implement consistent and frequent scanning of systems and technology that look for weaknesses and ensure all systems are operating with the most up-to-date software, including antivirus software.
- Manage user access through systems and procedures that require strong passwords and authentications and limits employee access to only those systems necessary to accomplish their tasks.
- Implement systems that are able to identify and prevent unauthorized or harmful traffic and develop and employ best practices for the remote use of systems (e.g., Virtual Private Network connection (VPN)).

In conclusion, while the creation and implementation of a comprehensive cybersecurity program can be challenging and expensive, the immediate and long-term consequences of a successful attack can be significant. Damage to a registrant's reputation and its relationship with both current and future clients and investors can be difficult to repair and as a result, registrants should utilize all available resources, including the Security and Exchange Commission's Cybersecurity Spotlight webpage and alerts issued by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, to develop and maintain an internal cybersecurity program that is adaptable and reactive to constantly shifting threats. Furthermore, registrants should continue to assess the effectiveness of the cybersecurity programs of every vendor and service provider that maintains a record of fund sensitive information.

MEET THE AUTHORS

Stacie L. Lamb

Associate

+1 312 569 1146
Chicago
stacie.lamb@faegredrinker.com

Diana E. McCarthy

Partner

+1 215 988 1146
Philadelphia
diana.mccarthy@faegredrinker.com

Services and Industries

Investment Management

Investment Management Compliance

Government and Regulatory Affairs

Privacy, Cybersecurity & Data Strategy