The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

**MEMO# 32598**

July 13, 2020

# OCIE Publishes Risk Alert on Ransomware

[32598]

July 13, 2020 TO: ICI Members
Chief Compliance Officer Committee
Chief Risk Officer Committee
Operations Committee SUBJECTS: Cybersecurity RE: OCIE Publishes Risk Alert on Ransomware

Last Friday, July 10th, the SEC's Office of Compliance Inspections and Examinations (OCIE) published its latest Risk Alert, which relates to ransomware.[1] According to this four-page document, "OCIE has observed an apparent increase in sophistication of ransomware attacks on SEC registrants," including broker-dealers, investment advisers, and investment companies.[2] In such attacks, the perpetrators behind the attacks typically demand a ransom to either "maintain the integrity and/or confidentiality of customer data or for the return of control over registrant systems." In light of these threats, the Risk Alert both encourages registrants to monitor cybersecurity alerts published by the Department of Homeland Security and Infrastructure Security Agency (CISA) and provides observations of OCIE that may assist registrants "in their consideration of how to enhance cybersecurity preparedness and operational resiliency to address ransomware attacks."

## CISA's Alert

As noted in the Risk Alert, on June 30, 2020, CISA published an alert on ransomware. This short (1-2 page) Alert updates an Alert that CISA originally released on February 18, 2020.[3] It includes a one-paragraph overview of "threat actor techniques" and corresponding mitigations and, in bullet form, it discusses how an attack occurred and lists actions firms are encouraged to consider as part of their risk-based assessment for mitigating such attacks.

## OCIE's Observations

The measures mentioned in the Risk Alert that OCIE has observed that may help a registrant mitigate a ransomware attack include:

- **Assessing, Testing, and Periodically Updating Incident Response and Resiliency Policies and Procedures, and Plans.** Such activities should include planning responses to a variety of cyber scenarios including ransomware and other denial of service attacks.

- **Operational Resiliency.** This involves firms understanding how their operations may continue if their primary system is unavailable.
- **Awareness and Training Programs.** The focus of this is on training employees about cyber risks and threats. This might also include conducting phishing exercises to help employees identify phishing email.
- **Vulnerability Scanning and Patch Management.** Firms may want to consider implementing proactive vulnerability and patch management programs that ensure timely patching and automatic updating of anti-virus and anti-malware solutions. Firms may additionally want to (i) conduct regular scans of their systems for vulnerabilities and (ii) upgrade their anti-malware capability.
- **Access Management.** Cyber defense should include ensuring that a firm's access controls are configured to ensure, on an ongoing basis, that users' access to the firm's systems and users' privileges are limited to those necessary to accomplish their tasks.
- **Perimeter Security.** The Risk Alert discusses the importance of perimeter security capabilities necessary to control, monitor, and inspect all incoming and outgoing network traffic to prevent unauthorized or harmful traffic. Perimeter security also includes activities such as firewalls, intrusion detection systems, email security, and web proxy systems with content filtering.

The Risk Alert reminds registrants that the SEC has focused on cybersecurity issues for many years and that cybersecurity has been key examination priority for OCIE. As evidence of this, the Risk Alert notes that, in addition to the current Risk Alert, OCIE has published other Risk Alerts on this topic and the SEC maintain a "Cybersecurity Spotlight" webpage that provides cybersecurity-related information and guidance.[4]

Tamara K. Salmon
Associate General Counsel

**endnotes**

[1] *See Cybersecurity: Ransomware Alert,* OCIE Risk Alert (July 10, 2020), which is *available at:* https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf.

[2] Though not mentioned in this Risk Alert, while such attacks may be "sophisticated," such attacks typically occur via a phishing email that an employee opens, which then provides the attacker access to the firm's systems.

[3] CISA's Alert AA20-049A is *available at:* https://us-cert.cisa.gov/ncas/alerts/aa20-049a.

[4] The Cybersecurity Spotlight is *available at* www.sec.gov/spotlight/cybersecurity. The Risk Alerts OCIE has previously issued related to cybersecurity can be found in the list of all Risk Alerts OCIE has issued. These are available at www.sec.gov/ocie under the "Risk Alert" tab.

should not be considered a substitute for, legal advice.