The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 30712

May 22, 2017

SEC Publishes Risk Alert Relating to the WannaCry Ransomware Attack

[30712]

May 22, 2017 TO: ICI Members
Chief Compliance Officer Committee
Chief Information Security Officer Advisory Committee
Small Funds Committee
Technology Committee SUBJECTS: Compliance
Cybersecurity
Investment Advisers
Technology & Business Continuity RE: SEC Publishes Risk Alert Relating to the WannaCry Ransomware Attack

On May 17th, the National Examination Program of the SEC's Office of Compliance Inspections and Examinations published a Risk Alert relating to their review of registrants' cybersecurity preparedness in the wake of the recent WannaCry attacks that affected organizations in over 100 countries.[1] According to the Risk Alert, OCIE's staff examined 75 registrants consisting of broker-dealers and investment management firms (which consisted of both SEC-registered investment advisers and funds). While the staff observed a wide range of information security practices, procedures, and controls among these registrants, the 2-page Risk Alert highlights three observations from their review, which they believe "may be particularly relevant to small firms." These three are:

- **Cyber-risk Assessment** – According to the staff, 5% of broker-dealers and 26% of investment firms examined did not conduct periodic risk assessments of critical systems to identify cybersecurity threats, vulnerabilities, and potential business consequences;
- **Penetration Testing** – 5% of broker-dealers and 57% of investment management firms they examined did not conduct penetration tests and vulnerability scans of critical systems; and
- **System Maintenance** – While 100% of the broker-dealers and 96% of the investment management firms had processes to ensure regular system maintenance, 10% of the broker-dealers and 4% of the investment management firms had "a significant number of critical and high-risk security patches that were missing important updates."

The Risk Alert notes guidance and updates published by the SEC that firms may want to consider when addressing cybersecurity risks and response capabilities. Links to this

information, which consists of the *IM Guidance Update: Cybersecurity Guidance* (April 2015) and information about OCIE's two cybersecurity initiatives (in 2014 and 2015) and its 2016 Risk Alert relating to its Cybersecurity Examination Initiative, can be found in footnote 6 to the Risk Alert.

Importantly, the Risk Alert concludes with the following: "The staff recognizes that it is not possible for firms to anticipate and prevent every cyber-attack. The staff also notes that appropriate planning to address cybersecurity issues, including developing a rapid response capability is important and may assist firms in mitigating the impact of any such attacks and any related effects on investors and clients."

Tamara K. Salmon
Associate General Counsel

endnotes

[1] *See CYBERSECURITY: RANSOMWARE ALERT,* (Volume VI, Issue 4) National Examination Program Risk Alert, OCIE (May 17, 2017), which is available at: https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf.
