Published on *The National Law Review* https://natlawreview.com

OCIE Issues Risk Alert on Critical Systems Following "WannaCry" Ransomware Attack

Article By:

Investment Services Group

On May 17, 2017, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert to highlight the importance of conducting penetration tests and vulnerability scans on critical systems and implementing system upgrades on a timely basis in response to the widespread ransomware attack known by the names of "WannaCry," "WCry" or "Wanna Decryptor" (WannaCry).

The Risk Alert notes that the hacker or hacking group behind the attack infected the computers of numerous organizations across hundreds of countries with a malicious software that encrypts the computer users' files and demands payment of ransom to restore access to the locked files. The Risk Alert encourages investment management firms and broker-dealers to (1) review the alert on the ransomware attack published by the United States Department of Homeland Security's Computer Emergency Readiness Team (USCERT)1; and (2) evaluate whether applicable Microsoft patches for Windows XP, Windows 8, and Windows Server 2003 operating systems are properly and timely installed.

The Risk Alert cites OCIE's recent examination of 75 SEC-registered broker-dealers, investment advisers, and investment companies, assessing cybersecurity practices and preparedness, and notes that a number of the observations made following such examinations are relevant to the WannaCry ransomware incident, including the following:

•Cyber-risk Assessment: Five percent of broker-dealers and 26 percent of investment advisers and funds examined did not conduct periodic risk assessments of critical systems to identify cybersecurity threats, vulnerabilities, and the potential business consequences.

•Penetration Tests: Five percent of broker-dealers and 57 percent of investment advisers and funds examined did not conduct penetration tests and vulnerability scans on systems that the firms considered to be critical.

*System Maintenance: All broker-dealers and 96 percent of investment advisers and funds examined have a process in place for ensuring regular system maintenance, including the installation of software patches to address security vulnerabilities. However, ten percent of the broker-dealers and four percent of investment advisers and funds examined had a significant number of critical and high-

risk security patches that were missing important updates.

The Risk Alert also advises firms to consider the guidance and other materials issued by the Division of Investment Management and OCIE when assessing the effectiveness of cybersecurity programs and response capabilities.[2] Although the staff recognized that it is not possible for firms to anticipate and prevent every cyber-attack, the staff noted 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."

---

1 The US-CERT alert is available at: https://www.us-cert.gov/ncas/alerts/TA17-132A.

2 These materials include the Cybersecurity Guidance Update issued by the Division of Investment Management in April 2015 (available at: https://www.sec.gov/investment/im-guidance-2015-02.pdf), the Risk Alert issued by OCIE in April 2014 on its cybersecurity initiative (available at: https://www.sec.gov/investment/im-guidance-2015-02.pdf), the Cybersecurity Examination Sweep Summary issued by OCIE in February 2015 (available at: https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf) and an update on OCIE's cybersecurity initiative, issued in September 2015 (available at: https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf).

National Law Review, Volume VII, Number 167

Source URL:https://natlawreview.com/article/ocie-issues-risk-alert-critical-systems-following-wannacry-ransomware-attack