NATIONAL EXAM PROGRAM
RISK ALERT

By the Office of Compliance Inspections and Examinations ("OCIE")[1]

Volume VI, Issue 4 **May 17, 2017**

This Risk Alert highlights the importance of conducting penetration tests and vulnerability scans on critical systems and implementing system upgrades on a timely basis.

CYBERSECURITY: RANSOMWARE ALERT

Starting on May 12, 2017, a widespread ransomware attack, known as WannaCry, WCry, or Wanna Decryptor, rapidly affected numerous organizations across over one hundred countries.[2] Initial reports indicate that the hacker or hacking group behind the attack is gaining access to enterprise servers either through Microsoft Remote Desktop Protocol (RDP)[3] compromise or the exploitation of a critical Windows Server Message Block version 1 vulnerability.[4] Some networks have also been affected through phishing emails and malicious websites. To protect against the WannaCry ransomware, broker-dealers and investment management firms are encouraged to (1) review the alert published by the United States Department of Homeland Security's Computer Emergency Readiness Team — U.S. Cert Alert TA17-132A — and (2) evaluate whether applicable Microsoft patches for Windows XP, Windows 8, and Windows Server 2003 operating systems are properly and timely installed.

OCIE's National Examination Program staff (the "staff") recently examined 75 SEC registered broker-dealers ("broker-dealers"), investment advisers ("advisers"), and investment companies ("funds") (collectively, "firms") to assess industry practices and legal, regulatory, and compliance issues associated with cybersecurity preparedness (the "Initiative").[5] The staff observed a wide range of information security practices, procedures, and controls across registrants that may be tailored to the firms' operations, lines of business, risk profile, and size. The staff observed firm practices during this Initiative that the staff believes may be particularly relevant to smaller registrants in relation to the WannaCry ransomware incident, including:

---

1 The views expressed herein are those of the staff of OCIE, in coordination with other staff of the Securities and Exchange Commission ("SEC" or "Commission"). The Commission has expressed no view on the contents of this Risk Alert. This document was prepared by the SEC staff and is not legal advice.

2 The WannaCry ransomware infects computers with a malicious software that encrypts computer users' files and demands payment of ransom to restore access to the locked files.

3 RDP provides remote display and input capabilities over network connections for Windows-based applications running on a server. RDP is designed to support different types of network topologies and multiple LAN protocols.

4 *See*, U.S. Department of Homeland Security/ U.S. Computer Emergency Readiness Team (US-CERT), Alert (TA17-132A), *Indicators Associated with WannaCry Ransomware* (May 12, 2017, last revised May 15, 2017) ("U.S. Cert Alert TA-132A").

5 *See*, OCIE *Examination Priorities for 2015* (Jan.13, 2015) and *National Exam Program Risk Alert, OCIE's 2015 Cybersecurity Examination Initiative* (Sept.15, 2015).

- **Cyber-risk Assessment:** Five percent of broker-dealers and 26 percent of advisers and funds (collectively, "investment management firms") 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 the investment management firms 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 management firms 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 management firms examined had a significant number of critical and high-risk security patches that were missing important updates.

The Division of Investment Management and OCIE have provided guidance and information that firms may wish to consider when addressing cybersecurity risks and response capabilities.[6] Similarly, for its member firms, the Financial Industry Regulatory Authority (FINRA) has created a webpage with links to cybersecurity-related resources, including a cybersecurity checklist for small firms and a report on cybersecurity practices that highlights effective practices for strengthening cybersecurity programs.[7] 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.

This Risk Alert is intended to highlight for firms the risks and issues that the staff has identified during examinations of broker-dealers, investment advisers, and investment companies regarding cybersecurity preparedness. In addition, this Risk Alert describes factors that firms may consider to (1) assess their supervisory, compliance and/or other risk management systems related to cybersecurity risks, and (2) make any changes, as may be appropriate, to address or strengthen such systems. These factors are not exhaustive, nor will they constitute a safe harbor. Factors other than those described in this Risk Alert may be appropriate to consider, and some of the factors may not be applicable to a particular firm's business. While some of the factors discussed in this Risk Alert reflect existing regulatory requirements, they are not intended to alter such requirements. Moreover, future changes in laws or regulations may supersede some of the factors or issues raised herein. The adequacy of supervisory, compliance, and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.

---

6 *See,* Division of Investment Management, *IM Guidance Update: Cybersecurity Guidance* (April 2015); OCIE, *National Exam Program Risk Alert, OCIE's 2014 Cybersecurity Initiative* (April 15, 2014), *National Exam Program Risk Alert, Cybersecurity Examination Sweep Summary* (Feb. 3, 2015), and *National Exam Program Risk Alert, OCIE's 2015 Cybersecurity Examination Initiative* (Sept. 15, 2015).

7 *See* FINRA, *Topic Page: Cybersecurity* (last visited May 16, 2017).