Weil

Private Equity Alert

OCIE Publishes Risk Alert Regarding Cybersecurity Examination Initiative for Registered Investment Advisers and Broker-Dealers

By David Wohl and Paul Ferrillo

Continuing its focus on cybersecurity issues, on September 15, 2015, the SEC's Office of Compliance Inspections and Examinations (OCIE) published a Risk Alert announcing guidance pertaining to the upcoming second round of cybersecurity examinations aimed at registered investment advisers and broker-dealers, which examinations will involve testing to assess implementation of firm procedures and controls. OCIE stated that its Cybersecurity Examination Initiative (the Initiative) is designed to build on its previous cybersecurity exams and guidance,[1] and to assess cybersecurity preparedness in the securities industry, including firms' ability to protect client information. In particular, the Initiative will focus on the following areas:

Governance and Risk Assessment: Examiners may assess whether registrants have cybersecurity governance and risk assessment processes relative to the key areas of focus discussed below. Examiners also may assess whether firms are periodically evaluating cybersecurity risks and whether their controls and risk assessment processes are tailored to their business. Examiners also may review the level of communication to, and involvement of, senior management and boards of directors.

Access Rights and Controls: Firms may be particularly at risk of a data breach from a failure to implement basic controls to prevent unauthorized access to systems or information, such as multifactor authentication or updating access rights based on personnel or system changes. Examiners may review how firms control access to various systems and data via management of user credentials, authentication, and authorization methods. This may include a review of controls associated with remote access, client logins, passwords, firm protocols to address client login problems, network segmentation, and tiered access.

Data Loss Prevention: Some data breaches may have resulted from the absence of robust controls in the areas of patch management and system configuration. Examiners may assess how firms monitor the volume of content transferred outside of the firm by its employees or through third parties, such as by email attachments or uploads. Examiners also may assess how firms monitor for potentially unauthorized data transfers and may review how firms verify the authenticity of a client request to transfer funds.

Vendor Management: Some of the largest data breaches over the last few years may have resulted from the hacking of third party vendor platforms. As a result, examiners may focus on firm practices and controls related to

vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms. Examiners may assess how vendor relationships are considered as part of the firm's ongoing risk assessment process as well as how the firm determines the appropriate level of due diligence to conduct on a vendor.

Training: Some data breaches may result from unintentional employee actions such as a misplaced laptop, accessing a client account through an unsecured internet connection, or opening messages or downloading attachments from an unknown source. Examiners may focus on how training is tailored to specific job functions and designed to encourage responsible employee and vendor behavior. Examiners also may review how procedures for responding to cyber incidents under an incident response plan are integrated into regular personnel and vendor training.

Incident Response: Examiners may assess whether firms have established policies, assigned roles, assessed system vulnerabilities, and developed plans to address possible future cybersecurity events. This includes determining which firm data, assets, and services warrant the most protection to help prevent attacks from causing significant harm.

We note that several areas of focus correspond to known cybersecurity breaches and methods by which attackers have been successful, like the exfiltration of passwords and the exfiltration and use of access information for individuals with heightened administrative privileges. Given the plethora of known software vulnerabilities discovered in 2014 and the first half of 2015, OCIE's emphasis on timely patching certainly is a reasonable "ask" in the present cybersecurity environment. Finally, as 91% of all data breaches have some element of human interaction (whether intentional or just an employee's inadvertently "clicking on the link"[2]), OCIE's emphasis on employee training is well placed.

The full text of the Risk Alert, including a sample request for information and documents to be used by OCIE in the upcoming exams, can be found at http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf. In light of the Initiative and Risk Alert, registered investment advisers and broker-dealers are urged to review their cybersecurity policies and procedures to ensure that they are prepared for an OCIE examination in this area.

1. *See* April 15, 2014 OCIE Cybersecurity Initiative, available at http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.
2. *See* "Wham, Bam, Thank You Spam: Please Don't Click on the Link," available at http://corpgov.law.harvard.edu/2015/05/17/wham-bam-thank-you-spam-dont-click-on-the-link/.

Private Equity Alert is published by the Private Equity practice group of Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

The Private Equity group's practice includes the formation of private equity funds and the execution of domestic and cross-border acquisition and investment transactions. Our fund formation practice includes the representation of private equity fund sponsors in organizing a wide variety of private equity funds, including buyout, venture capital, distressed debt, and real estate opportunity funds, and the representation of large institutional investors making investments in those funds. Our transaction execution practice includes the representation of private equity fund sponsors and their portfolio companies in a broad range of transactions, including leveraged buyouts, merger and acquisition transactions, strategic investments, recapitalizations, minority equity investments, distressed investments, venture capital investments, and restructurings.

If you have questions concerning the contents of this issue, or would like more information about Weil's Private Equity practice group, please speak to your regular contact at Weil, or to the editors, practice group leaders or contributing authors:

Authors:

Paul Ferrillo (NY)	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372
David Wohl (NY)	Bio Page	david.wohl@weil.com	+1 212 310 8933