CLIENT UPDATE

SEC RELEASES CYBERSECURITY EXAMINATION ROADMAP

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Michael P. Harrell
mpharrell@debevoise.com

Min Lee
mjlee@debevoise.com

Joseph W. Weissman
jweissman@debevoise.com

WASHINGTON D.C.
Kenneth J. Berman
kjberman@debevoise.com

Robert B. Kaplan
rbkaplan@debevoise.com

Satish M. Kini
smkini@debevoise.com

The SEC is digging into cybersecurity. On April 15, 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a Risk Alert announcing it would conduct examinations of more than 50 registered broker-dealers and registered investment advisers (a category that includes advisers to private equity, hedge and other private funds as well as mutual funds) to assess the registrants' cybersecurity preparedness. The Risk Alert describes areas on which OCIE will focus and includes a sample document request. Broker-dealers and registered investment advisers should review the Risk Alert in anticipation of a possible examination. In addition to serving as a roadmap for firms preparing for a possible examination by OCIE, the Risk Alert identifies the cybersecurity processes and features that firms should consider in assessing and improving their cybersecurity programs.

INCREASING SEC FOCUS ON CYBERSECURITY

The Commission's announced Examination Priorities for 2014 include technology and cybersecurity. On March 26, 2014, Commission Chair Mary Jo White led a Cybersecurity Roundtable where she and others from the private and public sectors discussed cybersecurity risks faced by financial market participants and public companies, as well as the challenges of sharing information about cyber risks with the government.

OCIE is the branch of the SEC that conducts regular exams of registered firms to monitor for compliance with the securities laws. OCIE examinations can lead to a variety of outcomes, including deficiency letters issued to registrants, referrals to the SEC's Division of Enforcement, and (as appears to be the main goal here) the collection and assessment of information that may support future policy initiatives by the Commission. Even what begins as a routine exam therefore can have serious effects, for the particular registrant under scrutiny and more broadly.

Following up on the Cybersecurity Roundtable, on April 15, 2014, OCIE issued its Risk Alert. OCIE declared that the upcoming examinations are part of the Commission's initiative "to assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats." OCIE's examinations will focus on:

- cybersecurity governance,
- identification and assessment of cybersecurity risks,
- protection of networks and information,
- risks associated with remote customer access and funds transfer requests,
- risks associated with vendors and other third parties,
- detection of unauthorized activity, and
- experience with certain cybersecurity threats.

USING THE SEC'S RISK ALERT AS A ROADMAP

OCIE's nine-page sample document request asks firm to describe, among other things, the frequency of their testing cybersecurity processes and controls; whether they protect against distributed denial of service ("DDoS") attacks; and how they manage risks associated with vendors and other third parties. The document request also asks firms to provide a comprehensive list of cyber incidents (e.g., malware, DDoS attacks, network breaches) discovered since January 1, 2013, and whether those events were reported to law enforcement, government agencies or industry organizations.

Like the Framework for Improving Critical Infrastructure Cybersecurity put out in February by the Department of Commerce's National Institute of Standards and Technology ("NIST"), the Risk Alert provides insight into what the government views as fundamental elements of a good cybersecurity program. Also like the NIST framework, the SEC's document request suggests an increasing emphasis on sharing information about

cyber risks outside of your organization – a complex issue that involves questions of confidentiality as well as security.

The Risk Alert follows up on the Commission's Identity Theft Flags Rules, which we discussed in a prior Client Update. Among other things, the Identity Theft Red Flag Rules require a broker or investment adviser that falls within the scope of the rules to implement a program that includes policies and procedures designed to identify identity theft red flags, detect their occurrence and respond appropriately. One of the questions in the recent Risk Alert's sample document request asks whether the firm has updated its written supervisory procedures to reflect the Identity Theft Red Flags Rules. If not, the firm is expected to provide an explanation.

SEC registrants would be well-advised to review the sample document request carefully, and then take steps to address any gaps that the review might expose in the firm's cybersecurity practices. Whether or not you are one of the 50 firms that will actually undergo an OCIE cybersecurity exam, the issuance of the Risk Alert is an opportunity to get ahead of the curve with respect to the emerging governmental standards in this critical area.

* * *

Please do not hesitate to contact us with any questions.

April 22, 2014