

SEC Issues Cybersecurity Risk Alert

April 22, 2014

On April 15, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a [Risk Alert](#) concerning its initiative to assess the cybersecurity preparedness of the securities industry. The Risk Alert states that OCIE will conduct examinations of more than 50 registered broker-dealers and investment advisers in order to identify areas where the SEC and the industry "can work together to protect investors and our capital markets from cybersecurity threats." To facilitate compliance, the Risk Alert includes a sample information request ("Request") that outlines the following areas where OCIE sees risk and will focus its examinations:

1. Identification of Risks/Cybersecurity Governance
2. Protection of Firm Networks and Information
3. Risks Associated with Remote Customer Access and Funds Transfer Requests
4. Risks Associated with Vendors and Other Third Parties
5. Detection of Unauthorized Activity
6. Experiences with Certain Cybersecurity Threats.

The Request provides a detailed roadmap of factors that firms may wish to consider in assessing their supervisory, compliance, and risk management systems. The 28 factors listed include several questions relating to:

- network security,
- physical security,
- periodic cybersecurity risk assessments,
- contracting with and monitoring vendors and other third parties,

- cybersecurity roles and responsibilities for employees and managers, and
- cybersecurity insurance.

The Risk Alert follows closely on the heels of the SEC's Cybersecurity Roundtable held on March 26, during which Chair Mary Jo White stated that the SEC's "formal jurisdiction over cybersecurity is directly focused on the integrity of our market systems, customer data protection, and disclosure of material information." Although the Risk Alert focuses on registered broker-dealers and investment advisers, other SEC-regulated entities that maintain client accounts or directly process customer transactions on an application-way basis may find it prudent to review the factors identified in the Risk Alert and keep a close eye on how these examinations play out in the coming year.

Authored By



Richard T. Choi

Related Practices

[Consumer Finance](#)

[Cybersecurity and Privacy](#)

[Financial Services Regulatory](#)

[Securities Litigation and Enforcement](#)

[Securities Transactions and Compliance](#)

[Technology](#)

Related Industries

[Technology](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.

