BRYAN CAVE
A Broader Perspective
Bulletin

Securities Litigation & Enforcement Client Service Group and
Investment Management Practice

To: Our Clients and Friends February 4, 2015

SEC Issues Cybersecurity Exam Observations

On February 3, 2015, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert summarizing its findings following examination of the preparedness of 57 broker-dealers and 49 investment advisory firms to address legal, regulatory and compliance challenges related to cybersecurity. These examinations grew out of the SEC's Cybersecurity Examination Initiative which began last year. *See* "OCIE Cybersecurity Initiative" (April 15, 2014): http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

As part of the exam, OCIE reviewed, among other items, each firm's culture generally, as well as specifically, their policies, procedures, and oversight mechanisms related to cybersecurity issues. OCIE examiners also looked at each firm's procedures for identifying risks; the nature and extent of network-level safeguards for protecting client information and firm infrastructure; each firm's ability to identify and evaluate risks presented by the use of third-party vendors; risks associated with client remote access and external fund transfer requests; and each firm's ability to detect and prevent unauthorized activity. Beyond evaluating firms in these general areas, OCIE examiners also interviewed key personnel regarding these issues, as well as any firm policies or protocol related to the reporting of a cyber-breach.

Perhaps most reflective of the magnitude of this particular issue, 88% of the broker-dealers and 74% of the examined advisers reported that they have been the subject of a cyber-related incident. OCIE's exam observations can be summarized as follows:

- 93%[1] of brokerage firms and 83% of advisory firms have written information security policies.
- The vast majority of brokerage firms (88%) and about half (53%) of advisors defer, at least to some extent to published cybersecurity risk management standards, such as those published by the National Institute of Standards and Technology ("NIST"), the International Organization for Standardization ("ISO"), and the Federal Financial Institutions Examination Council ("FFIEC").

[1] Percentages are based on the universe of 57 brokerage firms and 49 advisory firms examined.

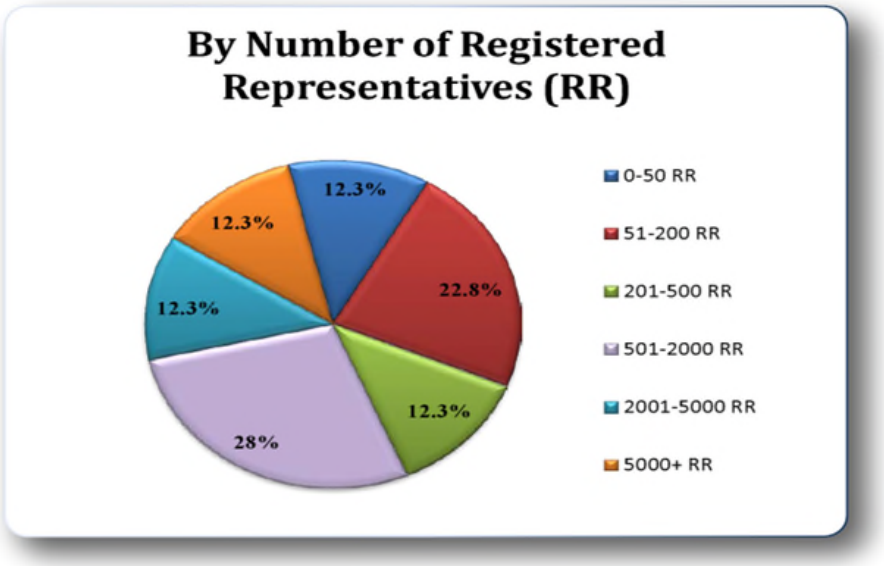
- 89% of brokerage firms and 57% of the advisors conduct periodic audits to determine compliance with information security policies and procedures.
    - A comparable percentage of firms have written business continuity plans for responding to cyber-attacks or intrusion but most (70% of brokerage firms and 87% of advisors) do *not* address potential responsibility for client losses associated with cyber incidents.
- The vast majority of examined brokerage firms (93%) and advisory firms (79%) conduct periodic risk assessments, on a firm-wide basis, to identify cybersecurity threats, vulnerabilities, and potential business consequences.
    - Only 84% of broker-dealers and far fewer advisory firms (32%) apply their cybersecurity policies, procedures and requirements to their vendors.
    - 72% of brokerage firms incorporate requirements relating to cybersecurity into their vendor contracts, while in contrast, only 24% of advisors did so. It appears to be the exception that any of the firms require information security training for vendors notwithstanding their access to the firm's network (51% for brokerage firms and only 13% of advisory firms).
- Receipt of fraudulent transfer requests via email impacted more than half of the broker-dealers (54%) and just under half of the advisers (43%).
    - Most firms reported these types of fraudulent emails to the Financial Crimes Enforcement Network (FinCEN) through the filing of a Suspicious Activity Report (SAR), but a negligible percentage notified law enforcement.
    - About 25% of the broker-dealers incurring losses related to fraudulent emails attributed those losses to a failure to follow identity authentication procedures. Similarly, the one adviser that reported a loss also noted that its employees had deviated from its identity authentication procedures.
- About half of brokerage firms examined collaborate with other firms through the use of information-sharing networks regarding best practices. Many of the broker-dealers identified the Financial Services Information Sharing.
- Mapping of technology resources was identified by the vast majority of the examined entities as an important cybersecurity strategy.
    - 96% of brokerage firms and 92% of advisors mapped their physical devices and systems.
    - For software applications the percentages were 91% and 92%, respectively.
    - Network resources, connections, and data flows were mapped by 97% of brokerage firms and 81% of the advisory firms.
    - Among brokerage firms, 91% mapped connections to firm networks from external sources, as compared to 74% of advisors.
    - Hardware, data, and software were mapped by 93% of brokerage firms and 60% of the advisors.
    - Logging capabilities and practices were tracked by 95% of brokerage firms and 68% of the advisors.
- Virtually all firms (98% of examined broker-dealers and 91% of advisers) make use of data encryption.

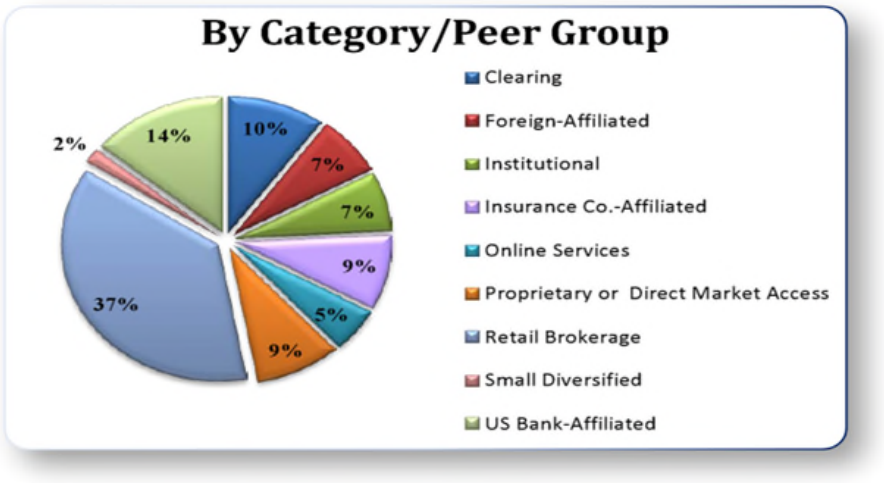
- 68% of the examined brokerage firms have a designated Chief Information Security Officer ("CISO"), while less than a third of the advisers (30%) have designated a CISO.
- Finally, just over half (58%) of examined brokerage firms purchase cybersecurity insurance, while a much smaller percentage (21%) of advisory firms do so.

As noted in our prior alert, cybersecurity is an Exam Priority for the SEC in 2015 – a point reiterated in this Risk Alert. Moreover, the Financial Industry Regulatory Authority also released its Report of Cybersecurity Practices, setting forth specific guidance for its members, which is covered in a separate Client Alert.

The *SEC National Exam Program Risk Alert*, Volume IV, Issue 4 on the *Cybersecurity Examination Sweep Summary* (Feb. 3, 2015) is available online.

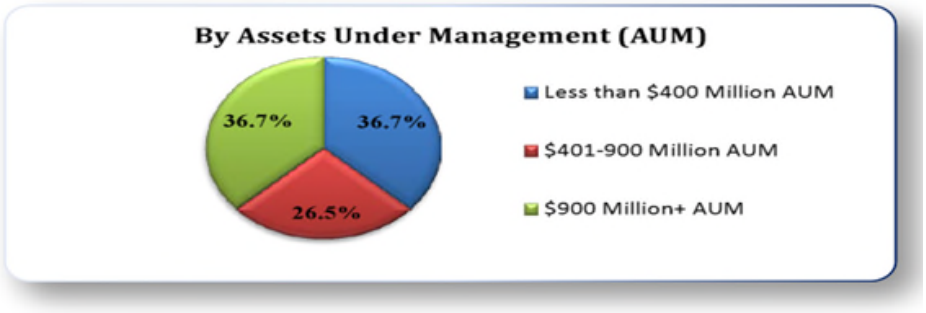
Breakdown of Examined Brokerage Firms (data is rounded)[2]

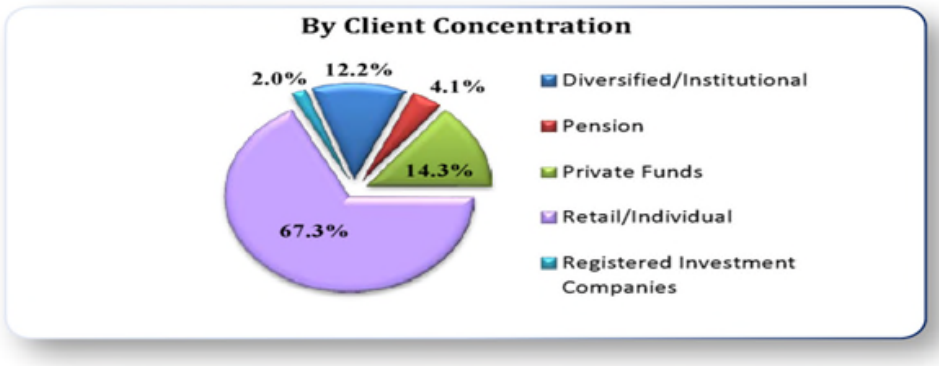




[2] Source: The *SEC National Exam Program Risk Alert*, Volume IV, Issue 4 on the *Cybersecurity Examination Sweep Summary* (Feb. 3, 2015)

Breakdown of Examined Investment Advisors (data is rounded)[3]





For questions or further information on this topic, please speak to your Bryan Cave contact, a member of our Securities Litigation and Enforcement or Investment Management teams, or the authors of this bulletin:

Rick Kuhlman
Partner, St. Louis
314-259-2820
rick.kuhlman@bryancave.com

Jason Kempf
Associate, St. Louis
314-259-2306
jason.kempf@bryancave.com

[3] Source: The *SEC National Exam Program Risk Alert*, Volume IV, Issue 4 on the *Cybersecurity Examination Sweep Summary* (Feb. 3, 2015)