Simpson Thacher

Memorandum

SEC and FINRA Report on Cybersecurity Sweep Examinations—Broker-Dealers Better Positioned than Advisers; SEC Issues Cybersecurity Guidance Update

May 13, 2015

The SEC issued a National Exam Program risk alert summarizing OCIE's cybersecurity examination sweep of advisers and broker-dealers on February 3, 2015 (SEC Risk Alert). On the same day, FINRA issued its report on cybersecurity practices of broker-dealers, based on its own sweep examination (FINRA Report). Neither the SEC Risk Alert nor the FINRA Report creates any new rules or legal obligations, but each provides insight into current industry practice.

Many commentators have interpreted the reported results as a sign that the industry is on top of cybersecurity issues, but OCIE specifically included cybersecurity controls among its examination priorities for 2015. Additionally, at various industry conferences and panels, members of the SEC's Division of Enforcement have mentioned the possibility of future enforcement actions relating to cybersecurity. A closer look at the SEC Risk Alert and FINRA Report reveals that broker-dealers may be in a better position than advisers in dealing with the anticipated increase in regulatory scrutiny of cybersecurity practices (although we of course are not expressing a view as to whether brokers are actually better positioned to prevent cyber-attacks than advisers). While that may not be surprising, given the significantly greater access brokers have to personal identifying information, advisers may nonetheless benefit from considering implementation of certain practices that have already been embraced by broker-dealer.

SEC Risk Alert

The SEC Risk Alert was the most recent step in the agency's ongoing cybersecurity initiative, which was formally announced in April 2014. During its sweep, OCIE examined 57 registered broker-dealers and 49 registered advisers. The SEC report indicates that OCIE attempted to capture a cross-section of each industry—the examined broker-dealers varied by number of registered representatives and types of services

offered, while the advisers varied by amount of assets under management, client-type and whether they held custody of client assets.

The SEC report outlines the areas targeted in the sweep examination:

- Identifying risks related to cybersecurity;
- Establishing cybersecurity governance, including policies, procedures and oversight processes;
- Protecting firm networks and information;
- Identifying and addressing risks associated with remote access to client information and funds transfer requests;
- Identifying and addressing risks associated with vendors and other third parties; and
- Detecting unauthorized activity.

Written policies/procedures

In summarizing OCIE's observations, the SEC Risk Alert begins by noting that the vast majority of examined broker-dealers (93%), but fewer advisers (83%), had adopted written cybersecurity policies/procedures. In evaluating compliance with written policies/procedures, broker-dealers (89%) were much more likely to conduct periodic audits than advisers (57%). Similarly, broker-dealers (88%) are much more likely to refer to well-known cybersecurity risk management standards in developing their cybersecurity practices, such as the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO) and the Federal Financial Institutions Examination Council (FFIEC), than advisers (53%). Also according to the report, broker-dealers (93%) are more likely than advisers (79%), to conduct periodic cybersecurity risk assessments and consider them in establishing practices.

Vendors

In some of the most high-profile cybersecurity incidents (e.g., the Target breach), third-party vendors have been the gateway for attackers to access a company's systems. In the mutual fund arena, boards are increasingly asking advisers about their diligence and oversight of vendor cybersecurity practices. Thus, the disparity found in OCIE's report between broker-dealer and adviser practices with respect to cybersecurity is notable. As discussed above, broker-dealers are more likely than advisers to conduct periodic risk assessments regarding their cybersecurity practices. With respect to vendors, broker-dealers (84%) are significantly more likely to require vendors to conduct periodic risk assessments than advisers (32%). Similarly, broker-dealers (72%) are much more likely to incorporate cybersecurity provisions into contractual agreements with vendors than advisers (24%) and broker-dealers (51%) are more likely to conduct cybersecurity training for vendors who have access to their networks than advisers (13%).

FINRA Report

As outlined above, broker-dealers generally appear to be better positioned for future OCIE examinations or SEC enforcement initiatives related to cybersecurity than advisers. In light of that observation, advisers may benefit from some of the results and best practices stated in the FINRA Report, which focuses on the practices of broker-dealers.

Metrics

The FINRA Report states that almost all broker-dealers (95%) use metrics to assess cybersecurity performance. Examples of metrics cited in the FINRA Report are: distributed denial of services attacks; network intrusions; data theft; encryption coverage (e.g., portable devices, e-mail, etc.); Adobe and Microsoft patch coverage; anti-virus coverage; and employee training (both initial and ongoing).

Firms then set a threshold for certain metrics and manage their activities accordingly. The FINRA Report provides the example of a firm setting a threshold of keeping 95% of its computers up-to-date on Adobe and Microsoft patches (i.e., less than 90 days old). If the firm falls below that threshold, it would escalate the issue for prompt resolution. The FINRA Report suggests that cybersecurity metrics can be useful in developing cybersecurity practices, as the discussions and decisions about what to track, where to set thresholds and organizational reporting for issues may lead to more well defined policies/procedures.

Inventories

Both the SEC Risk Alert and FINRA Report espouse the importance of asset inventories as a foundational tool in establishing sound cybersecurity practices. Generally, advisers' practices were in line with broker-dealers with respect to conducting firm-wide inventories of physical devices and systems and software platforms and applications, but advisers lagged behind in taking inventories of: network resources; connections and data flows; connections to firm networks from external sources; hardware, data and software; and logging capabilities and practices. The FINRA Report notes that many broker-dealers maintain strong policies to ensure that all assets are subject to centralized review and control.

Vendor contracts

As discussed in connection with the SEC Risk Alert, broker-dealers are much more likely to incorporate cybersecurity provisions into contractual arrangements with vendors. The FINRA Report offers several examples of standard contract provisions for vendors that will have access to firm systems, addressing topics such as: non-disclosure/confidentiality; data storage, retention and delivery; breach notification responsibilities; right to audit clauses; vendor employee access limitations; use of sub-contractors; and vendor obligations upon contract termination.

Subsequent SEC Guidance Update

On April 28, 2015, the SEC Division of Investment Management issued a guidance update on cybersecurity. Citing OCIE's cybersecurity report, the guidance update begins by emphasizing the need for funds and advisers to review their cybersecurity practices. The tenor of the guidance update indicates that the SEC views cybersecurity as an ongoing compliance endeavor, where a "set it and forget it" approach might be inadequate. Among other considerations for funds and advisers, the guidance update recommends implementing written policies and procedures (citing Rule 38a-1), and training, with respect to the following measures:

- Funds and advisers should conduct periodic assessments of:
  - Technology systems and the nature, sensitivity and location of information collected, processed and/or stored;
  - Internal and external threats and vulnerabilities;
  - Controls and processes;
  - The potential impact of systems being compromised; and
  - Governance and management of cybersecurity risk.
- Funds and advisers should engage in strategic planning to prevent, detect and respond to cybersecurity threats, including implementation (and testing) of:
  - Access controls, such as authentication and authorization methods, firewalls and keeping software up-to-date;
  - Data encryption;
  - Restrictions on the use of removable storage devices, such as flash drives;
  - Software that monitors for unusual events;
  - Information sharing with vendors and industry groups, such as the Financial Services – Information Sharing and Analysis Center;
  - Data backup; and
  - Response planning.

Future SEC Examinations and Enforcement

The SEC has increasingly cited cybersecurity as an examination and enforcement priority. As noted, OCIE has listed cybersecurity compliance and controls among its 2015 examination priorities, and members of the SEC Staff have been dropping hints of impending enforcement activity in this area. Given the general lack of

existing guidance and the evolving nature of this area, talk of potential enforcement actions is a bit alarming. For example, at an industry conference in early February, SEC Office of Market Intelligence Chief Vincente Martinez raised some eyebrows when he suggested that the SEC can rely on Regulation SP (Privacy), Regulation S-ID (Identify Theft) and Regulation SCI (Systems Compliance Integrity) to bring an enforcement action if a registered investment adviser's cybersecurity practices are deficient. Additionally, the SEC's recent guidance update states that the SEC Staff believes that funds and advisers have compliance obligations under federal securities laws related to preventing, detecting, responding and mitigating cybersecurity threats, citing again to Regulation SP and Regulation S-ID and also referencing Codes of Ethics rules, prohibitions on open-end funds from suspending shareholder redemptions and advisers' general fiduciary duty to clients to avoid the risk of being unable to provide advisory services.

We believe that any talk of enforcement is, at best, premature. Even if the OCIE report accurately reflects a greater attention to cybersecurity on the part of broker-dealers, as compared to advisers, it does not suggest a lack of attention. Indeed, for a variety of reasons, including high profile hacks, our experience suggests that the industry is taking its obligations with regard to cybersecurity very seriously. We note, in this regard, the creation of industry working groups to combat cyber threats. A high-profile enforcement action has the benefit, from the regulator's perspective, of focusing attention on an issue that is being ignored by regulated entities. However, cybersecurity is already a focus of industry participants, and enforcement actions in this area would in our view push the industry towards focusing on compliance policies at the expense of focusing on operational mechanisms to prevent cyber attacks in the first place.

If you have any questions or would like additional information, please do not hesitate to contact any member of the Firm's Privacy and Cybersecurity Practice or Registered Funds Practice.

Simpson Thacher Worldwide

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
600 Travis Street, Suite 5400
Houston, TX 77002
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
1155 F Street, N.W.
Washington, D.C. 20004
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3919 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
West Tower, Mirae Asset Center 1
26 Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000