DORSEY

DORSEY+WHITNEY LLP

# SEC's Latest Cybersecurity Risk Alert Identifies Elements of Robust Policies and Procedures

On August 7, 2017 the Securities and Exchange Committee ("SEC") Office of Compliance Inspections and Examinations ("OCIE") released yet another cybersecurity Risk Alert entitled, "Observations from Cybersecurity Examinations." In this most recent Risk Alert, OCIE details its findings from its Cybersecurity 2 Initiative, which involved the examination of 75 firms, including broker-dealers, investment advisers, and investment companies between September 2015 and June 2016. Following its 2014 Cybersecurity 1 Initiative, the Cybersecurity 2 Initiative set out to assess industry practices and legal, regulatory and compliance issues associated with cybersecurity preparedness, focusing in greater depth on validation and testing of procedures and controls. As the Risk Alert sets forth a list of elements OCIE considers to be robust policies and procedures, it should be used as a check list for registrants in assessing the adequacy and effectiveness of their cybersecurity compliance program in light of their business risks.

The SEC has made cybersecurity a priority in recent years as more cyber-attacks threaten the industry. In addition to being named as a National Examination Program priority, cybersecurity has been a focus on the SEC's outreach program. The SEC shared the results from its Cybersecurity 1 Initiative in its February 2015 Risk Alert entitled, "Cybersecurity Examination Sweep Summary." In May of this year, OCIE put out a Risk Alert regarding the ransomware called "WannaCry" in which OCIE initially shared its observations from its Cybersecurity 2 Initiative to provide guidance to registrants for strengthening cybersecurity programs and protecting against the ransomware. Beyond its exam program and outreach, the SEC's Enforcement Division has also been focusing on the matter by bringing cases against investment advisers and broker-dealers for cybersecurity-related violations. On all fronts the SEC is trying to get the message out that cybersecurity is one of the greatest risks facing the financial services industry and registrants must ensure their compliance programs address the risks posed by cyberattacks.

The Cybersecurity 2 Initiative exams focused on the following areas: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor

## Related Capabilities

- Securities & Financial Services Litigation & Enforcement
- Privacy & Social Media

management; (5) training; and (6) incident response. Generally, the staff found the cybersecurity preparedness of the firms they examined had improved since its Cybersecurity 1 Initiative testing in 2013 and 2014. Some of the improvements noted in the Cybersecurity 2 Initiative findings include:

- *Testing and monitoring*:
  - 95% of broker-dealers and 74% of advisers and funds conduct periodic risk assessments of vulnerable systems;
  - Nearly all of the firms had plans in place for addressing incidents;
  - 95% of broker-deals and 43% of advisers and funds conducted penetration tests and vulnerability scans on firm-identified critical systems; and
  - All firms examined had some form of control in place to monitor data loss of personally identifiable information.

- *Policies and Procedures*:
  - Nearly all firms had policies and procedures in place to address cyber-related business continuity planning and Regulation S-P;
  - All of the advisers and funds maintained policies, procedures, and standards related to verifying the authenticity of a customer or shareholder requesting to transfer funds; and
  - Nearly all broker-dealers and most advisers and funds had specific policies addressing Regulation S-ID.

The Risk Alert also discussed some issues noted during the testing, including policies and procedures not reasonably tailored to the firm, firms' actual practices not reflecting their written policies and procedures, and Regulation S-P issues among firms that did not appear to conduct system maintenance. Finally, the Risk Alert provided details of what the SEC considers elements of "robust policies and procedures." These included:

- *Maintenance of an inventory of data, information, and vendors*. Policies and procedures included a complete inventory of data and information, along with classifications of the risks, vulnerabilities, data, business consequences, and information regarding each service provider and vendor, if applicable.
- *Detailed cybersecurity-related instructions*. Examples included:
  - Penetration tests: policies and procedures policies included specific information to review the effectiveness of security solutions.
  - Security monitoring and system auditing: policies and procedures regarding the firm's information security framework included details related to the appropriate testing methodologies.
  - Access rights: requests for access were tracked, and policies and procedures specifically addressed modification of access rights, such as for employee on-boarding, changing positions or responsibilities, or terminating employees.
  - Reporting: policies and procedures specified actions to undertake, including who to contact, if sensitive information was lost, stolen, or unintentionally disclosed/misdirected.

- *Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities*. Examples included:
  - Vulnerability scans of core IT infrastructure were required to aid in identifying potential weaknesses in a firm's key systems, with prioritized action items for any

concerns identified.
  - Patch management policies that included, among other things, the beta testing of a patch with a small number of users and servers before deploying it across the firm, an analysis of the problem the patch was designed to fix, the potential risk in applying the patch, and the method to use in applying the patch.

- *Established and enforced controls to access data and systems*. For example, the firms:
  - Implemented detailed “acceptable use” policies that specified employees’ obligations when using the firm’s networks and equipment.
  - Required and enforced restrictions and controls for mobile devices that connected to the firms’ systems, such as passwords and software that encrypted communications.
  - Required third-party vendors to periodically provide logs of their activity on the firms’ networks.
  - Required immediate termination of access for terminated employees and very prompt (typically same day) termination of access for employees that left voluntarily.

- *Mandatory employee training*. Information security training was mandatory for all employees at on-boarding and periodically thereafter, and firms instituted policies and procedures to ensure that employees completed the mandatory training.
- *Engaged senior management*. The policies and procedures were vetted and approved by senior management.

Along with federal regulations that address cybersecurity preparedness, investment advisers and broker-dealers should also watch out for new state cybersecurity regulations aimed at financial institutions. New York was the first state to put out such cybersecurity regulations, which came into force on March 1 of this year. Although investment advisers are not covered entities under the New York law, some may have affiliated outside business activities that are covered by the regulations. Earlier this summer, Colorado adopted a similar set of cybersecurity rules which do cover investment advisers. Those rules became effective July 15, 2017.

In sum, SEC registrants should review OCIE’s suggested "robust policies and procedures" in light of their business and consider whether their current written policies and procedures are adequate and effectively implemented. Registrants should also be prepared to respond to OCIE exam requests regarding these policies and procedures and the registrant’s related testing. Dorsey attorneys are available to assist with any corresponding questions or concerns.