The SEC's Cybersecurity Priorities for Registered Investment Advisers—Looking Back to Anticipate the Road Ahead

March 11, 2021

Earlier this week, Debevoise published an overview of the SEC's Division of Examination Priorities for 2021. Today, we're taking a deeper dive into one aspect of those priorities: cybersecurity as it applies to Registered Investment Advisers ("RIAs"). The recent publication of the SEC's 2021 Division of Examination Priorities (the "2021 Priorities") presents an opportunity to look back at the cybersecurity work of the SEC in 2020 and speculate about the SEC's examination and enforcement priorities for data protection in the coming year for RIAs.

The SEC's press release announcing the 2021 Priorities succinctly sets out its cybersecurity focus as follows:

- Safeguarding customer accounts and preventing account intrusions, including verifying an investor's identity to prevent unauthorized account access.
- Overseeing vendors and service providers.
- Addressing malicious email activities, such as phishing or account intrusions.
- Responding to incidents, including those related to ransomware attacks.
- Managing operational risk as a result of dispersed employees in a work-from-home environment.

LOOKING BACK AT 2020

Enforcement

In terms of cybersecurity enforcement in the RIA space, 2020 was a quiet year for the SEC. We wrote about two enforcement actions, neither of which involved core cybersecurity issues. The first was a settlement with JonesTrading for failing to preserve business-related text messages. The second was a settlement with BlueCrest Capital

Management for not disclosing to investors its use of an algorithmic trading tool. For core cybersecurity issues, the SEC's actions against Voya Financial Advisors ("VFA") (2018) and Options Clearing Corp and Virtu Americas LLC ("Virtu") (2019) remain the key benchmarks for understanding its enforcement priorities.

VFA involved bad actors posing as contractors who called the company's help desk claiming to need account passwords reset. The SEC found that help desk employees violated various company policies in resetting the passwords, including failing to check the phone numbers from which the bad actors were calling against a list of known "bad" numbers. The case was notable, in part, because it was the first time the SEC charged a violation of the Identity Theft Red Flags Rule.

In Virtu, the company attempted to keep its alternative trading system ("ATS") volume below the threshold requiring compliance with Regulation Systems Compliance and Integrity ("Regulation SCI"). To do so, Virtu implemented a volume monitoring system that was designed to discontinue trading in particular securities before the trading volume exceeded the Regulation SCI threshold. The system did not work and Virtu's ATS volume required compliance with Regulation SCI. The SEC charged Virtu for violating, among others, the requirement to "establish, maintain, and enforce written policies and procedures" to secure SCI systems and their operational capacity.

Guidance

The SEC's Division of Examinations (the "Division") was very active on cybersecurity issues in 2020.

- In January, it released its 2020 Examination Priorities Memo, stating that the Division would "continue to prioritize information security in each of its five examination programs." The key areas of focus included: (1) governance and risk management; (2) access controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response and resiliency.

- Also in January 2020, the Cybersecurity and Resiliency Observations was released, which emphasized the importance of senior level engagement for an effective cybersecurity program, including in providing strategic guidance and oversight.

- The Risk Alert on Ransomware was released in July 2020 and underscored the continuing threat posed by these types of attacks. The Division emphasized the importance of training to detect and avoid phishing emails, which are often the initial vector for these attacks, and encouraged RIAs to adopt ransomware-specific response plans.

- In August 2020, the Select COVID-19 Compliance Risks and Considerations for Broker-Dealers and Investment Advisers was released, in which the Division recommended "that Firms pay particular attention to the risks regarding access to systems, investor data protection, and cybersecurity," suggesting RIAs conduct gap assessments of their policies and procedures.

- In September 2020, the Division issued a September 2020 Risk Alert on Credential Compromise. Credential compromise attacks—sometimes called "credential stuffing" or "list validation" attacks—occur when a bad actor acquires the usernames and passwords for a company's online customer accounts from an unrelated data breach, and attempts to use those login credentials on other systems. These attacks work because many customers reuse username and password combinations across multiple websites. Some cybersecurity professionals do not view these attacks as cyber incidents of the company because they involve the compromise of customer (not employee) accounts, and the initial breach that exposed the credentials occurs elsewhere. The Division's guidance sets forth its view on the responsibility of companies to prevent successful credential stuffing of customer accounts. The Alert encouraged firms to conduct "[s]urveillance of the dark web for lists of leaked user IDs and passwords, and performance of tests to evaluate whether current user accounts are susceptible to credential stuffing attacks." Also in September 2020, the New York Attorney General announced a settlement with Dunkin' Donuts for failing to respond adequately to a series of a credential stuffing attacks.

- Although not limited to cybersecurity issues, the Division's November 2020 OCIE Observations: Investment Adviser Compliance Programs called out RIAs for failing to address issues that had been identified in risk assessments, conducting incomplete assessments that failed to identify key risks and having policies—including policies associated with information security—that were insufficiently tailored to the firm's needs.

THE ROAD AHEAD AND KEY TAKEAWAYS

The SEC's 2021 Priorities highlight the increased risks associated with work-from-home protocols and vendor management, both of which we have discussed in depth in the last year here and here. And for the first time, the 2021 Priorities specifically call out ransomware attacks and safeguarding customer accounts, both of which we have analyzed here and here.

1. Close Out Major Issues

If you have already taken steps to identify risks, make sure that you have a plan to remediate them. Prioritizing risks is an acceptable approach, but the SEC is likely to be less tolerant of delinquent risk remediation going forward.

2. Ransomware Preparations

If your Incident Response Plan ("IRP") does not already include a ransomware protocol, now is the time to consider adding one. In addition, consider reviewing your roster of incident response vendors for both cybersecurity and operation resiliency. For ransomware attacks, in addition to the traditional cybersecurity firms that are called in when an incident occurs, firms are increasingly proactively engaging vendors that specialize in negotiating with ransomware hackers, obtaining cryptocurrency should payment become necessary, and assisting with systems restoration after a decryption key is delivered.

3. Senior-Level Engagement

Review how senior executive leadership and the board are involved in cyber issues. Check for policies and systems that would facilitate leadership's timely engagement on critical cyber issues.

4. Tabletop Exercises

Tabletop exercises or other kinds of simulation exercises where decision-makers run through specific scenarios (such as a ransomware attack) and test response decisions, escalation procedures and communication strategies can be very useful in making your cyber preparedness plans more robust.

5. Employee Training

The SEC repeatedly has identified phishing as a key initial vector for many sophisticated follow-on attacks, and so companies should make sure that they are adequately training employees on how to recognize and report phishing attempts. Some firms have adopted a button that employees can use to flag phishing emails to the information security department. Training should include ways to reduce the new cybersecurity risks that arise from remote work arrangements.

6. Credential Stuffing

To reduce the risk of credential stuffing and customer account takeovers, firms should consider preventative measures such as: employing a trusted device program for customers that triggers multifactor authentication for attempted logins from new devices and dark web monitoring for compromised passwords. For employee accounts, many firms have adopted multifactor authentication for all remote access, as well as

policies that prevent employees from using the same password for both their corporate email and any other online account.

7. Cybersecurity Vendor Management

Companies should consider creating a cybersecurity risk management framework for vendors that have direct access to sensitive company data or are critical to the firm's core operation. Such a framework may include identifying high-risk factors, a cybersecurity vendor questionnaire and a set of risk mitigating options to use with vendors that have a high risk of experiencing a cybersecurity incident that could materially impact the firm.

To subscribe to the Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Avi Gesser
agesser@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Tricia Reville
pmreville@debevoise.com

Mengyi Xu
mxu@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com