The SEC's Cyber Priorities and Four Additional Ways for Companies to Reduce Regulatory Risk

July 29, 2021

Earlier this year, we wrote about the SEC's cybersecurity priorities. Since then, the SEC announced a settlement with First American Title Insurance and Services ("First American") for violating Rule 13a-15(a) of the Exchange Act, and issued a voluntary request for information to a number of companies in connection with the SolarWinds cyber attack ("Voluntary Request"). In this Debevoise Update, we discuss these developments and provide an update on ways that companies can reduce their cybersecurity regulatory risk.

The First American Settlement. According to the SEC's order, First American's security personnel identified a security vulnerability exposing over 800 million document images during a penetration test in January 2019. Some of those exposed documents contained sensitive personal data such as customer Social Security numbers and financial information dating back to 2003. The vulnerability was not remediated or reported to information security managers according to First American's policies. In May 2019, a cybersecurity journalist notified First American of the same vulnerability and First American issued a press statement and submitted an 8-K. According to the order, First American senior executives responsible for these public statements were not made aware that the company's IT personnel had previously identified this vulnerability and failed to fix it, and therefore "lacked certain information to fully evaluate the company's cybersecurity responsiveness and the magnitude of the risk" posed by the vulnerability at the time of the company's disclosures.

The SEC accordingly found that First American failed to maintain disclosure controls and procedures designed to ensure that all available relevant information concerning the vulnerability was analyzed for disclosure in the company's SEC filings. As part of this settlement, First American agreed to a cease-and-desist order and to pay a $487,616 penalty.

The SolarWinds Voluntary Request. The SEC's Voluntary Request was directed at companies potentially impacted by the cyber attack on SolarWinds and sought, among other things, (1) information about how each company was impacted by the incident, if at all, and (2) any remedial measures taken in connection with the attack. The Voluntary

Request also appears to offer amnesty to companies who addressed outstanding disclosure violations in response to the attack prior to responding to the Voluntary Request.

The Voluntary Request reaffirms the SEC's expectation, as set forth in the 2018 Commission Statement and Guidance, that companies tailor their public disclosures to particular cybersecurity risks and incidents, and maintain disclosure controls and procedures that ensure that directors, officers, and cybersecurity personnel are made aware of any material cybersecurity risks faced by the company.

A company that engages in a robust response to a software-based attack should be able to list some of the following remedial measures in response to a regulatory inquiry:

- Installing new firewall rules to block traffic with servers running the affected software.
- Conducting a comprehensive search for any systems running the affected software.
- Shutting down all potentially impacted servers.
- Changing service account passwords for the affected software.
- Reviewing historical logs for traffic with the malicious servers.
- Engaging outside experts to assist in the assessment of the risks and remediation.
- Reaching out to critical vendors with a written questionnaire to confirm that they were not adversely impacted, and tracking the responses.
- Rebuilding and upgrading the servers in accordance with any applicable government guidance.
- Obtaining indicators of compromise from the software provider or CISA and adding them to their endpoint detection tools.

Takeaways. In our previous post on SEC's cybersecurity priorities, we listed seven takeaways based on recent SEC enforcement actions and guidance: (1) Close Out Major Issues, (2) Ransomware Preparations, (3) Senior-Level Engagement, (4) Tabletop Exercises, (5) Employee Training, (6) Credential Stuffing and (7) Cybersecurity Vendor Management. Based on the First American settlement and the Voluntary Request, we add the following four takeaways to that list:

1. **Effective Disclosure Controls**. In its press release on First American, the SEC stressed that issuers must ensure that information important to investors is reported up the corporate ladder to those responsible for making disclosures in a timely manner. In its FAQs concerning the Voluntary Request the SEC reiterated its expectation that companies provide tailored disclosures of their cybersecurity incidents and risks. Companies should implement procedures to make sure that significant cybersecurity and technology issues are properly escalated within the organization and promptly shared with legal and compliance functions.

2. **Follow Your Cyber Policies**. The SEC emphasized that First American did not follow its own cybersecurity policies when it failed to remediate the vulnerability within its predetermined deadline. The NYDFS made a similar observation in its Statements of Charges against First American relating to the same incident. Cybersecurity policies should be tested and followed, and should not be merely aspirational.

3. **The Value of Penetration Testing**. The vulnerability at issue for First American had been embedded in its EaglePro application since 2014. Robust penetration testing programs that include applications containing personal information can often uncover these kinds of vulnerabilities—which companies must then promptly address.

4. **Be Prepared for Supply Chain/Software Attack**. The recent Kaseya ransomware attack demonstrates that supply-chain cyber incidents like the cyber attack on SolarWinds are not unique events. Having received sundry responses to its Voluntary Request, the SEC is now familiar with the hallmarks of the robust response to a software cyber attack, and is likely to expect companies to:

    - Quickly assess whether they are running the impacted software.
    - Block traffic with servers running the affected software.
    - Determine whether there has been any unauthorized activity in connection with the impacted software.
    - Reach out to their critical vendors to assess if they have been impacted.
    - Disable, update and rebuild in accordance with any applicable government guidance.

* * *

Please do not hesitate to contact us with any questions.

To subscribe to the Data Blog, please click here.

The authors would like to thank Debevoise & Plimpton Summer Associate Katie McCarty for her contribution to this blog post.

NEW YORK

Avi Gesser
agesserl@debevoise.com

Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

Suchita Mandavilli Brundage
smbrundage@debevoise.com