Fall Cybersecurity Enforcement Update: State and Federal Regulators Increase Scrutiny on Victims of Cyberattacks

We have written here previously about the dramatic increase in cyberattacks on companies of all types since the start of the COVID-19 pandemic. Indeed, by some estimates, ransomware attacks have increased over 90% during the first half of 2021 compared to the same period last year. As these and other types of cyberattacks have increased, various federal and state regulators have correspondingly stepped up efforts to investigate and bring enforcement actions – which often include large fines – against companies that are perceived to have been negligent in their cybersecurity efforts. Two of the most active agencies in cybersecurity enforcement have been the New York Department of Financial Services (NYDFS) and the United States Securities & Exchange Commission (SEC), both of which have made important announcements regarding cybersecurity compliance in the past few months.

New York Department of Financial Services

As discussed in prior blog posts, in 2021 the NYDFS has announced several enforcement actions stemming from violations of its first-in-the-nation Cybersecurity Regulations. In addition, on June 30, 2021, NYDFS announced new guidance on ransomware prevention for covered entities.

As a part of its guidance, NYDFS provided a list of controls that it encouraged covered entities to implement. The list includes:

- Implementing employee training in cybersecurity awareness and anti-phishing techniques
- Executing a vulnerability and patch management program

- Using multifactor authentication and strong passwords
- Employing privileged access management to safeguard credentials for privileged accounts
- Using monitoring technologies to detect and contain intruders
- Segregating and testing backups to ensure that critical systems can be restored in the event of an attack
- Preparing a ransomware-specific incident response plan that is tested by senior leadership

On the same date, NYDFS also published an industry letter further detailing these suggested controls, as well as discussing the possibility of increased reporting requirements for covered entities. In particular, NYDFS noted that covered entities "should assume that any successful deployment of ransomware on their internal network should be reported[.]"

Notably, NYDFS already requires regulated entities to report data breaches as promptly as possible and "within 72 hours at the latest," pursuant to 23 NYCRR § 500.17(a). NYDFS appears to have used the industry letter to announce that the agency is considering clarifying its reporting requirements to expressly require that ransomware incidents be reported.

The industry letter further reiterated the requirement that regulated companies implement the controls listed above, as well as other mitigation efforts, whenever possible. Controls specifically relevant to mitigating a ransomware attack include the requirement to maintain comprehensive, segregated backups that allow recovery in the event of a ransomware attack. See 23 NYCRR §§ 500.03(e), (f), and (n).

NYDFS also reiterated that regulated entities must have an incident response plan that explicitly addresses ransomware attacks. *See* 23 NYCRR § 500.16. And, after drafting comprehensive response procedures, the plan should be tested, and the testing should include senior leadership.

Securities & Exchange Commission

In the past month, the SEC has announced multiple high-profile enforcement actions against businesses that were found to have inadequate cybersecurity programs, policies, or responses.

On August 16, 2021, the SEC announced that a multinational company agreed to pay $1 million to settle charges related to a 2018 cyber intrusion involving the theft of student records, including dates of birth and email addresses, as well as inadequate disclosure controls and procedures. The SEC alleged that the company's disclosures to customers following the data breach were inaccurate and potentially misleading. Furthermore, the SEC took issue with the fact that the company claimed to have had "strict protections" for cybersecurity in place, when, in fact, it allegedly failed to patch the critical vulnerability until six months after it was notified of the issue.

Additionally, on August 30, 2021, the SEC announced the settlement of three other cybersecurity enforcement actions. In all three cases, the SEC alleged that the companies' cloud-based email accounts had been taken over by malicious actors, which had resulted in the exposure of personal identifying information of numerous customers and clients. The SEC also took issue with the companies' disclosures and alleged lack of preparation against such attacks. The fines for the three companies ranged between $200,000 and $300,000.

These recent enforcement actions are a sign of regulatory agencies' increasing willingness to scrutinize and penalize lax cybersecurity practices. They serve as yet another reminder that companies should review their existing policies and practices and implement revised and additional controls in areas they determine to be lacking.

About the Author: Peter Baldwin

Peter Baldwin draws on his experience as a former federal prosecutor to counsel clients facing government investigations and cybersecurity issues. View Peter's full bio on the Faegre Drinker website.

About the Author: Grayson Harbour

Grayson Harbour is an associate in the firm's Labor & Employment practice group. Read Grayson's full bio on the Faegre Drinker website.

Subscribe and Receive Alerts to New Articles

SUBSCRIBE

September 7, 2021

Written by: Peter Baldwin and Grayson Harbour

Category: Cybersecurity

Tags: cyberattack, cybersecurity, incident response plan, NYDFS, SEC