ALM | LAW.COM

Legaltech® news

How to Stay on Top of Cybersecurity Disclosures as SEC Ramps Up Enforcement

By Stephenie Gosnell Handler, David Woodcock & Vivek Mohan, Gibson Dunn
May 4, 2023

It is no secret among public companies and their counsel that the US Securities and Exchange Commission has steadily adopted a more aggressive stance on cybersecurity controls and disclosure and incident response recordkeeping. SEC Senior Counsel Arsen Ablaev recently highlighted the Commission's cybersecurity priorities at the annual Incident Response Forum Masterclass. SEC Chair Gary Gensler also emphasized risks in cyber and information security in the March 29 budget hearing with the House Appropriations Committee, and endorsed U.S. President Joe Biden's request to earmark a record $2.4 billion in funding for the regulator in 2024. Last month saw yet another example of the SEC's mounting focus on cyber disclosures as an enforcement priority with the announcement that cloud computing company Blackbaud agreed to pay a $3-million civil penalty to settle administrative charges for alleged "materially misleading disclosures" about a 2020 ransomware attack.

As we foreshadowed in our 2023 U.S. Cybersecurity and Data Privacy Outlook and Review, the increase in SEC enforcement resources (e.g., doubling the size of its Crypto Assets and Cyber Unit Ablaev sits in), in combination with the promulgation of cybersecurity risk management, strategy, governance, and incident disclosure rules Ablaev confirmed will be finalized in coming months, signal that cybersecurity will continue to be an area of heightened enforcement activity for the SEC. In light of these developments, it is critical companies take stock of

their cyber hygiene policies and incident response protocols, and not only manage cybersecurity risks and prevent attacks, but also respond to them with proper disclosures.

Ablaev at Incident Response Forum: SEC's Priorities and Blackbaud as a Masterclass In What Not To Do

While speaking in his personal capacity at the Incident Response Forum Masterclass on April 20, 2023, Ablaev touched on the SEC's cyber-enforcement priorities with respect to issuers. Referencing the rules that will soon be finalized, Ablaev said the SEC's priorities can be divided into three categories:

1. Flow of information: both internal information flow from CISOs (chief information security officers) up to the company's senior brass and board, as well as external information flow to investors;

2. More involvement and oversight by senior management, executives, and in some cases, company board, in risk management, cybersecurity hygiene, and incident response; and

3. More robust documentation and recordkeeping related to breaches and incident response, including transparent and ongoing disclosures of material cyber incidents.

On issuers' concern of disclosing information mid-breach, particularly if the vulnerability is yet to be resolved and intelligence about the incident drastically changes day to day, Ablaev said that is less of an issue today compared to five years ago.

"There is a shift from in the bunker-style communications on a cyber incident and towards a more transparent approach," according to Ablaev.

Determining materiality in the cyber context is a key consideration when choosing what to disclose publicly. Ablaev's advice on this front is to ask whether there is "a substantial likelihood that a reasonable investor would find the information important in making an investment decision (i.e., buying or selling or holding a security)."

The recent Blackbaud enforcement action is a primer on what not to do. A South Carolina-based publicly traded company, Blackbaud provides donor data management software to non-profit organizations.

According to the SEC order (the company neither admitted nor denied the SEC's findings):

- On May 14, 2020, Blackbaud's technology personnel detected unauthorized access to the company's systems.
- Two months later, Blackbaud announced the incident publicly and notified over 13,000 impacted customers, indicating the attacker did not access any donor bank account information or social security numbers.
- Within days of these statements, however, the company's technology and customer relations personnel learned the attacker had in fact accessed this information in an unencrypted form for many customers, but did not communicate this information to senior management.
- The company filed a Form 10-Q in August 2020 that discussed the incident, but failed to disclose the exfiltration of donor social security numbers and bank account numbers, and "misleadingly characterized the risk of exfiltration of such sensitive donor information as hypothetical."

The SEC's administrative order found that Blackbaud violated the anti-fraud provisions of the Securities Act (Sections 17(a)(2) and (3)) and other provisions of the securities laws requiring public companies to maintain adequate disclosure controls and procedures to ensure timely and accurate reporting of cybersecurity incidents. Blackbaud is also facing dozens of class action lawsuits related to the cyberattack, with its financial hit exceeding the insurance coverage it carries, according to a recent regulatory filing.

Companies Must Take Action Now

The SEC's stance, the *Blackbaud* settlement, and upcoming regulations offer several lessons relating to cybersecurity breaches.

Disclosure controls and procedures must encompass cybersecurity. The key issue for the SEC was that Blackbaud did not have disclosure controls or procedures designed to ensure that information relevant to cybersecurity incidents and risks were communicated to the company's senior management and other disclosure personnel, so relevant information related to the ransomware attack was never assessed from a disclosure perspective. The *Blackbaud* action echoes the SEC's Rule 13a-15(a) charges brought in June 2021 against First American Financial Corp. relating to disclosures concerning the company's discovery of a widespread cyber vulnerability. Public companies should anticipate that SEC staff will continue to focus on disclosure controls and procedures, especially procedures that give management the opportunity to consider timely disclosure of any known cybersecurity incidents and vulnerabilities as well as developments that have impacted prior disclosures. While Rule 13a-15 has for most of its existence been a tag-on charge, the SEC has recently given the rule new life and vigor.

Coordination between technical experts and disclosure decision-makers is key and should be documented. Although Blackbaud's cybersecurity experts were aware of the unauthorized access and exfiltration of donor bank account numbers and social security numbers by the end of July 2020, they failed to communicate the broader scope of the impacted data to the company's senior management responsible for disclosures. Moreover, the company did not have policies or procedures in place designed to ensure that such information flow occurred. Having a group including cybersecurity experts, reporting personnel, and legal counsel convene periodically and as needed to consider disclosure obligations is one way to ensure the appropriate information is captured and considered for disclosure. This process and decisions should be documented, so that if its conclusions are second-guessed, there is a record for defense.

Cybersecurity disclosures but must be monitored and updated for technical and factual developments. Coordination between technical experts and those who oversee the company's disclosures is key. The lack of communication between cybersecurity experts and Blackbaud's leadership shows that public statements must be scrutinized and re-vetted through the disclosure controls processes in evolving situations, where dynamic forensic investigations can result in new findings. It also demonstrates that companies need a fluid process for updating their risk factors. A disclosure that a possible risk may occur is likely to be insufficient or deemed misleading if the company has in fact suffered a cyber breach that the SEC deems to be material. This means having robust internal policies and procedures in place to report, escalate, and update breaches up the chain of command to ensure public disclosures are timely, accurate, and complete.

Companies should consult with counsel when making materiality assessments. The *Blackbaud* settlement, like *In re Pearson plc* we flagged last year, highlights the importance of carefully assessing the materiality of a cyberattack. In both cases, the SEC determined that the data breach was material based on the company's business and its user base, the nature and volume of the data exfiltrated, and the importance of data security to the company's reputation, as reflected in the company's existing risk disclosures. Consulting with counsel in making materiality assessments can help mitigate the risk when the government inevitably second-guesses materiality judgments.

The SEC's cybersecurity rulemaking will create even more fertile ground for enforcement investigations and matters. While those SEC proposed cybersecurity rules have yet to be finalized, the Blackbaud order hits many of the themes encompassed by the proposal. For instance, the proposal will require (1) early disclosure of material cyber incidents in the Form 8-K; (2) periodic disclosure of a company's policies and procedures to identify and manage cybersecurity risks; (3) disclosure of board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk; and (4) updates about previously reported material cybersecurity incidents. However the rules are finalized, companies can be sure that the core issues of disclosure controls and procedures and board oversight will be key areas of interest for SEC enforcement.

Stephenie Gosnell Handler is partner with Gibson Dunn's Cybersecurity & Data Innovation practice, based in DC. Vivek Mohan is partner with the Privacy, Cybersecurity and Data Innovation practice and co-chair of the firm's Artificial Intelligence practice, based in Palo Alto. David Woodcock is partner and co-chair of the firm's Securities Enforcement Practice Group, based in Dallas. Mashoka Maimona, who is licensed and admitted only in Ontario, contributed substantially to this article.

Reprinted with permission from the May 4, 2023 edition of the LEGALTECH NEWS © 2023 ALM Global Properties, LLC. All rights reserved. Further duplication without permission is prohibited, contact 877-256-2472 or reprints@alm.com. # LTN-5052023-43374