BRACEWELL

INSIGHTS

SEC Is Still Cyber Serious About Disclosures

August 19, 2021

*By: **Seth D. DuCharme** **Matthew G. Nielsen***

On the heels of the ***First American enforcement action and settlement***, this week, the SEC ***announced*** a settlement with Pearson plc in connection with a 2018 cyber breach. The SEC disclosed that Pearson, a London-based educational company, agreed to pay a $1 million penalty to settle charges that it misled investors about a breach involving the theft of millions of student records. The SEC's First American and Pearson settlements highlight the agency's increased focus on cybersecurity-related disclosures and should be nothing short of a wake-up call to all publicly traded companies.

In March 2019, Pearson was notified by the FBI that data stored on the system's server had been accessed and downloaded by a hacker using an unpatched vulnerability on the server. The vulnerability had been flagged as critical by the software manufacturer the previous September, and although a patch to fix the vulnerability was available, Pearson failed to implement it until after it learned of the breach, the SEC alleges.

Pearson created an incident response team and retained an outside vendor to investigate the breach. Analysis of the stolen data provided to Pearson showed that school administrator usernames and passwords has been exfiltrated, along with student names, birthdays, and email addresses. Pearson issued its semi-annual financial report to the SEC on July 26, 2019 and published a media statement a week later. The SEC found that Pearson made misleading statements and omissions in both public statements following the breach.

According to the agency, Pearson's 2019 semi-annual financial report referred to a data privacy incident as a "hypothetical risk, when, in fact, the 2019 cyber intrusion had already occurred." In the media statement issued that same month, Pearson stated that the breach "may" include dates of birth and email addresses, when the company knew for a fact that such records were stolen. The same statement by Pearson also omitted the fact that millions of student data, usernames, and passwords had been stolen. As the SEC noted, the data breach was material because the company acknowledged in its risk disclosures that its reputation and ability to retain and grow revenue depended upon its ability to protect personally identifiable information. The SEC also focused on Pearson's statement that the company had "strict protections" in place, when it actually took the company six months to patch the vulnerability. Like in First American, the SEC also claimed that Pearson did not have processes in place to ensure that information about the breach and security controls made its way to those making disclosures for the company.

“As the order finds, Pearson opted not to disclose this breach to investors until it was contacted by the media, and even then Pearson understated the nature and scope of the incident, and overstated the company's data protections,” said the Chief of the SEC Enforcement Division's Cyber Unit. “As public companies face the growing threat of cyber intrusions, they must provide accurate information to investors about material cyber incidents.”

As the top U.S. markets watchdog steps up enforcement around data breach and cybersecurity disclosures, public companies should consider several proactive measures:

- Review public disclosures and statements to confirm risk is described accurately;
- Be careful using conditional language when describing a breach to avoid misleading investors;
- Avoid making strong statements about data security postures that cannot be supported by evidence in addition to SEC enforcement, statements that mischaracterize could also bring scrutiny from the FTC; and
- Ensure that controls are in place that promptly escalate cyber incidents to those in charge of SEC reports so that proper disclosures are made.

The Pearson and First American orders will likely be followed by other SEC enforcement actions related to company knowledge about data breaches as compared to their cybersecurity disclosures. So far, the SEC has been fairly patient with public companies as a whole, as cyber risk disclosures have become more detailed and sophisticated. Indeed, this July, the SEC conducted a far-reaching enforcement sweep of SolarWinds customers, offering conditional amnesty for those who took corrective action and disclosed any material impact of the 2019 malware attacks. However, these recent orders suggest that the SEC is willing to take a more assertive posture when companies limit their cyber disclosures to “general risks,” failing to own up to actual cyber incidents and any associated specific risks. Bracewell attorneys are ready to help companies navigate the changing landscape around cyber disclosures and SEC enforcement.