Davis Polk

SEC sanctions company for hypothetical cyber risk factor when the company already had an incident

August 23, 2021 | Client Update | 3-minute read

The SEC filed an enforcement action against a company for disclosing the risk that it "could" have a data privacy breach when it knew it already had experienced a breach. The action also shows the importance of software patch management, which can significantly reduce the number of incidents.

On August 16, the Securities and Exchange Commission (SEC) announced a settlement with Pearson plc (Pearson), a London-based company that primarily provides educational publishing services to schools and universities, for making a misleading risk factor disclosure about data breaches. Pearson collected large volumes of student data and administrator log-in credentials, and learned in March 2019 that millions of rows of data had been stolen by a sophisticated threat actor. The company mailed a breach notice to customers in July 2019 but did not disclose the breach in its SEC filings. Instead, its next SEC filing included a statement that a data privacy incident was a risk that "could result" in a major breach.

The company received a media inquiry a few days later, and gave the reporter a statement the company had prepared months before. The statement said that the data breach "may" have involved certain types of information that the SEC asserts the company already knew were involved. The statement also referred to the incident as "unauthorized access" and "expos[ure of] data" instead of disclosing that data had been removed, and did not include all of the types of data at issue. The statement said that the company had strict protections in place, had fixed the issue, and had no evidence the information had been misused, even though it had failed to patch the vulnerability for six months and was using an outdated encryption algorithm.

The SEC alleged that both the SEC filing and the media statement were misleading, including because they characterized a known harm as a hypothetical risk. The SEC also said the company lacked adequate disclosure controls. Without admitting or denying the SEC's findings, the company agreed to pay a $1 million penalty.

Takeaways

The case has several important takeaways:

1. It can be problematic to describe cybersecurity and data privacy as hypothetical risks in SEC filings if a company already has experienced an incident.

2. Efforts to manage a news story through a media statement can lead to government sanctions if the statement is deemed misleading or incomplete in a material way.

3. The case provides some insight about the SEC's view of the materiality of cybersecurity disclosures. Here, the stock priced declined by a relatively modest 3.3% after the media statement (although the SEC alleged the statement was misleading and incomplete). To support its claim of materiality, the SEC also said that the company was in the business of collecting and storing large volumes of private data, and that the company had identified its ability to

protect this information as a risk factor.

4. Fourth, the case continues the SEC's focus on disclosure controls for cybersecurity issues, which we discussed in this prior client update.

Finally, and most simply, the case shows the need for diligent patch management. The SEC said that the company knew about the patch for the vulnerability for six months before implementing it. The simple step of applying software patches promptly can prevent many types of cybersecurity and data privacy incidents.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Matthew J. Bacal
+1 212 450 4790
matthew.bacal@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Angela T. Burgess
+1 212 450 4885
angela.burgess@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

Joseph A. Hall
+1 212 450 4565
joseph.hall@davispolk.com

Michael Kaplan
+1 212 450 4111
michael.kaplan@davispolk.com

Paul J. Nathanson
+1 202 962 7055
+1 212 450 3133
paul.nathanson@davispolk.com

Richard D. Truesdell, Jr.
+1 212 450 4674
richard.truesdell@davispolk.com