Client Update
How to Disclose a Cybersecurity Event: Recent Fortune 100 Experience

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Paul M. Rodel
pmrodel@debevoise.com

David M. Becker
dmbecker@debevoise.com

Brett M. Novick
bmnovick@debevoise.com

Benjamin R. Pedersen
brpedersen@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

Cybersecurity threats pose real challenges for any company, including the theft of valuable intellectual property and the reputational harm caused by losses of customer information. Attendant to the operational and financial challenges associated with cybersecurity threats, SEC reporting companies must also consider their disclosure obligations resulting from the risk or occurrence of any data breaches or other cybersecurity events.

During the period from January 2013 through the third quarter 2015, there were 20 reported incidents of major data breaches or cybersecurity events at Fortune 100 companies. While this number is without doubt a fraction of the total cybersecurity events experienced at these and similar companies during that time, a survey of these cybersecurity events, and the manner in which each of the 18 affected companies responded in their periodic filings with the SEC, is instructive. We have compiled a detailed database, comparing disclosure responses of these companies across a number of vectors in order to guide this complex process. This article provides a high-level comparison of the cybersecurity event disclosure we analyzed before, during and after the occurrence of material cybersecurity event.

The article is broken into two parts: first, we discuss considerations around initial public disclosure of the cybersecurity event by the affected Fortune 100 companies, and second, we discuss how the affected companies approached subsequent periodic reports and the need to update disclosure.

The bottom line is that most companies did not handle initial disclosure of a breach through a current report on a Form 8-K, instead deferring disclosures to the next periodic filing. Most companies did, however, update disclosures in the context of their annual report.

INITIAL DISCLOSURE

Current Reports

Following a cybersecurity event, the initial public announcement by the affected companies was typically made via press coverage, rather than in a current report on Form 8-K. The affected companies most often waited for their first subsequent periodic report (*i.e.*, Form 10-Q or Form 10-K) before including disclosure of the event in SEC filings. Companies that elected to disclose in a current report on Form 8-K most often did so where the breach involved customer financial information. In the initial period following a cybersecurity event, affected companies should also be mindful of selective disclosure issues and their obligations under Regulation FD.

When determining whether or not to report a cybersecurity event, in addition to materiality, registrants must also consider risks associated with drafting initial disclosure with incomplete data. For instance, in the immediate aftermath of a major breach, the "known" facts may represent a small piece of the cybersecurity risk mosaic, which can require significant forensic research to assemble. Companies electing to publicly disclose the occurrence of a cybersecurity event before completing a full investigation risk making incomplete, or, worse yet, inaccurate disclosure.

First Subsequent Periodic Report

After experiencing a cybersecurity event, registrants frequently use the first subsequent periodic filing to review existing risk factors related to cyber risks and to update these risk factors, if necessary. Where the first subsequent periodic filing following a cybersecurity event was a quarterly report, the affected companies were more likely to defer updating their risk factors, consistent with the generally infrequent practice of updating risk factors in quarterly reports. However, if the cybersecurity event was material to the affected company's business (and, in particular, if they had previously disclosed the cybersecurity event via a current report), it was more likely for the cyber risk factors to be addressed in the affected company's first subsequent quarterly report. On the other hand, if the first subsequent periodic report was an annual report, affected companies almost uniformly took the opportunity to update their cyber risk factors and, in most instances, referred specifically to the cybersecurity event.

SUBSEQUENT UPDATES

Risk Factor Updates

Even where the affected company had updated its cyber risk factors in its first quarterly report following the cybersecurity event, further updates were often included in the first subsequent annual report. In some cases, this may have been a result of particularly material breaches that required ongoing disclosure updates. However, many registrants view their annual report as an opportunity to update and tailor risk factors more generally, and the occurrence of an intervening cybersecurity event provides fodder for such fine tuning, including potentially adding specific reference to the cybersecurity event.

The affected companies did not generally engage in continued updating of disclosure in later quarterly reports following the initial disclosure, regardless of whether the initial disclosure was via a current report or a periodic filing. The exceptions to this observation can generally be explained by the severity of the related cybersecurity event, particularly where the event has had a lasting impact on the affected company's financial statements (*e.g.*, as a result of costs relating to litigation or regulatory responses).

Overall, we identified a trend of including specific reference to recent cybersecurity events in risk factors where applicable. However, some affected companies instead chose to disclose the types of risks associated with a previous cybersecurity event, without actually calling out the event. This decision may have been driven by the materiality of the cybersecurity event: the less material the event, the less the need to disclose with specificity. Other cyber risk factor trends included noting that both consumer data and employee data may be targeted, the risk of breaches at third parties that handle the registrant's data, internal procedures in place to protect data and detect breaches and disclosure regarding cyber insurance.

Other Updates

Disclosure related to cybersecurity at the affected companies was less frequently included outside of the risk factors section of quarterly and annual reports. When disclosure appeared elsewhere, the financial statement footnotes or the Management's Discussion and Analysis section were most frequent, though disclosure also occasionally appeared in the Legal Proceedings and Business disclosure. Often, disclosure in the body of a quarterly or annual report of an affected company was via cross-reference to the financial statement footnotes, underscoring that such disclosure generally flows from ongoing financial obligations related to cybersecurity events.

There were few instances of cybersecurity disclosure outside of current reports and periodic reports. In the event of a major business or financing transaction, it is possible that disclosure will be necessary as part of the description of that transaction, including the risks associated with consummating the transaction. In certain circumstances, cyber disclosure may also be included in the Proxy Statement following a cybersecurity event, for instance to discuss the formation of a committee to oversee cybersecurity risks. It will be interesting to observe this trend over time, as the SEC continues to focus on cybersecurity, and boards of directors become more involved in overseeing cyber-preparedness and in responding to cybersecurity events.

CONCLUSION

As illustrated by this summary of recent disclosure of cyber events at Fortune 100 companies, calibration of a registrant's disclosure response must take into account a number of variables (including all of the facts and circumstances particular to each registrant and each cybersecurity event), must be done on a case-by-case basis and must reflect that many key facts and circumstances may not yet be known with certainty.

Those companies seeking to mitigate the legal risks that can flow from untimely—or, worse, inaccurate—disclosures would do well to take stock of where their key information assets reside now, and how those assets are protected. That way, in a breach situation, the company may be able to more quickly ascertain whether information was accessed, the nature of the information (if any) that was accessed and the materiality of the breach.

* * *

Please do not hesitate to contact us with any questions.