CORPORATE COUNSEL
An ALM Website
corpcounsel.com | June 12, 2017

We've Been Hacked—What Do We Need to Disclose in Our SEC Filings?

By William Brady, Karen Neuman and Kara Harrington

It's the call that every general counsel dreads: *"We've been hacked."* In the face of an increasing threat, cybersecurity preparedness and incident response have become top priorities for corporate boards and general counsel. Smart companies have prepared by implementing comprehensive written information security plans (to minimize the potential for a cyber incident) and incident response plans that are regularly exercised and updated in order to facilitate crisis management and decision-making in the hours, days and weeks once an incident occurs. This article focuses on how to comply with potential reporting and other disclosure obligations.

U.S. SECURITIES AND EXCHANGE COMMISSION BUILDING IN WASHINGTON.

Photo by Diego M. Radzinschi/THE NATIONAL LAW JOURNAL

In the wake of a cyber incident, a general counsel is confronted with a flood of questions that must be answered quickly. What are our obligations under the patchwork of state, federal and international laws and regulations that may require reporting, especially if financial services or health information are impacted? What is the risk-benefit analysis of disclosing an incident to law enforcement? For public companies, another question is: What, if anything, do we have to disclose in our Securities and Exchange Commission (SEC) filings?

The answer to this last question cannot be separated from the various state law notification and reporting obligations that may apply in the event of an incident—in reality, if disclosure to a state attorney general or the company's customers is required, for instance, then that may well force the company's hand in terms of SEC disclosure. In any event, the SEC has made clear that it is stepping up its scrutiny of cyber incident disclosure; as the SEC's Acting Enforcement Director stated recently during a panel at the International Association of Privacy Professionals' Global Privacy Summit: "We've not brought an action in that space. Could I see a circumstance where we do? Absolutely."

Guidance issued by the SEC Division of Corporate Finance in October 2011 states that, "[a]lthough no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. In addition,

material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading."

But what is "material" ends up being far less clear, and there is plenty of room for a public company to determine in good faith that a specific cyber incident does not require separate disclosure. Where the obligation is unclear, a company's reluctance to disclose is understandable: Disclosure may highlight vulnerabilities, and will bring unwelcome attention from customers, regulators and others. The plaintiffs' bar will also circle, smelling the possibility of a class action, and they will not view the company and its managers as the victims.

It comes as little surprise, then, that the vast majority of companies conclude that no disclosure is necessary. Statistics compiled by Privacy Rights Clearinghouse and reported in the *Wall Street Journal* last fall bear this out: Just 95 of the roughly 9,000 public companies in the US have notified the SEC of a data breach since January 2010, yet across public and private companies in the same time period there were 2,642 breaches or hacks. Tatyana Shumsky, *Corporate Judgment Call: When to Disclose You've Been Hacked*, Wall Street Journal (Sept. 19, 2016). The SEC staff has made clear that they "are not looking to second-guess good faith disclosure decisions," and are "not looking for a slip on the banana peel." Jimmy Hoover, *SEC Suits Over Cyber Reporting Could Be On Horizon*, Law360 (April 20, 2017).

But the SEC is ready to act. For example, earlier this year, the SEC opened an investigation into Yahoo! Inc. following the company's disclosures in late 2016 of a 2014 data breach that compromised the data of at least 500 million users, as well as an August 2013 data breach that reportedly exposed the private information of more than 1 billion users. Aruna Viswanatha & Robert McMillan, *Yahoo Faces SEC Probe Over Data Breaches*, Wall Street Journal (Jan. 23, 2017). The takeaway: the SEC is going to focus on cases where there is a long lag between a major breach and disclosure, where there are questions about the company did to investigate and why customers were not notified.

So how can public companies meet their obligations and manage risk in this environment? Action should start prior to any incident, by having a good incident response plan in place that is tailored to the company's risk profile and organizational structure, and makes clear what the steps are and who should do what. Decision-making on reporting and disclosures should be assigned to a cross-functional crisis management team staffed by the General Counsel, CISO, CTO, CPO, CMO, Communications Chief and other stakeholders as appropriate who can recommend appropriate action to decision makers. The plan should be regularly exercised and ensure that relevant information is appropriately elevated to decision makers.

After an incident, among the first calls a general counsel should make is to outside counsel, to preserve privilege, tap strategic expertise about disclosure obligations, and assist with managing other aspects of the crisis. Assisted by outside counsel, companies must assess their reporting obligations under the patchwork of state, federal, and international laws, *including* any SEC disclosure obligations. For the SEC piece, companies must consider whether their existing risk disclosures adequately cover the incident—and if not, consider whether the risk disclosures must be updated to cover what happened. In making that assessment, the company will have to consider the materiality of the incident, which includes the potential impact on the business from customers, damage to the company's reputation and brand, and potential remedial costs and legal matters. Each situation will depend on the facts, but by planning ahead and arriving at a good faith disclosure decision, companies can help to contain the damage from an incident.

William Brady *is a partner in Goodwin Procter's litigation department and a member of its securities litigation and white-collar defense group.* ***Karen Neuman****, a partner in the firm's business litigation group and a member of its privacy and cybersecurity practice, is former Chief Privacy Officer with the U.S. Department of Homeland Security.* ***Kara Harrington*** *is an associate in the firm's litigation department.*