BARNES & THORNBURG LLP

Who's Watching The Watchdog? SEC Deals With Its Own Data Breach

September 25, 2017 | | SEC,The GEE Blog

Trace Schmeltz
Partner
Financial and Regulatory Litigation Group
Co-Chair, Fintech Co-Chair

On Sept. 20, SEC Chairman John Clayton announced that Wall Street's watchdog, the Securities and Exchange Commission (SEC), was the victim of a cyber hack in 2016. In what ironically amounts to the SEC's first significant disclosure of its own cybersecurity risks, Clayton stated: "In certain cases, threat actors have managed to access or misuse our systems." According to Clayton, "[i]n August 2017, the Commission learned that an incident previously detected in 2016 may have provided the basis for illicit gain through trading." Hackers apparently exploited a weakness in the SEC's Electronic Data Gathering, Analysis and Retrieving (EDGAR) system. EDGAR houses financial records for all of the companies listed on stock exchanges in the United States – including domestic and foreign securities issuers and some companies with publicly traded debt. Such data, says cybersecurity expert Morgan Wright, could have allowed hackers to manipulate markets and put upwards of $1 trillion in assets at risk by manipulating markets. The SEC's announcement is particularly ironic in light of the fact that, in 2011, the SEC's Division of Corporation Finance (Corp Fin) issued guidance to registrants regarding the need for, and how to think about, risk disclosures arising from cyberattacks. According to Corp Fin, as of 2011, the SEC had "observed an increased level of attention focused on cyber attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information." Based on this, the risks associated with such attacks (particularly to businesses with a significant online presence), and the costs associated with defending against and remediating the impact of cyberattacks, Corp Fin prescribed certain measures intended to ensure that the investing public understands the true costs of cyber crime. Corp Fin predicated its guidance on the idea that "registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption." In plain English, the higher the probability of a cyberattack that would have significant affects on a business, the greater the certainty that a registrant should disclose that information to its investors. And, the greater the likelihood that the registrant should be spending money (and disclosing the magnitude of such expenses, if material) to address those cyber risks. Under appropriate circumstances,

RELATED PRACTICE AREAS

Financial and Regulatory Litigation
Government Litigation
Securities and Capital Markets
White Collar and Investigations

Corp Fin recommended that registrants consider a disclosure of the "aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences" and even "[r]isks related to cyber incidents that may remain undetected for an extended period." It also noted that this assessment should be ongoing, particularly in light of increased risk from ever-changing cyberattacks. Corp Fin's guidance may be nothing more than varnish on Regulation S-K, which provides an in-depth analysis of what registrants need to include when filing forms under the Securities Act of 1933, the Exchange Act of 1934, and the Energy Policy and Conservation Act of 1975. But, because 2017 has seen an inordinate number of cyberattacks, details of which can be read in USA Today, The New York Times and Wired, now may be a good time for any company (whether a registrant with the SEC or not) to revisit its cybersecurity conventions. Indeed, in the past several weeks, Equifax, one of the "big three" credit reporting agencies, also announced that its site had been hacked. The cyberattack at Equifax exposed 124 million people's personal identifying information to misappropriation. And, yet, Equifax waited nearly five weeks to disclose the hack to the public – potentially in violation of Reg S-K and the Corp Fin guidance. To compound matters, after the hack was discovered, several Equifax executives sold Equifax stock before the issue was disclosed, a typical no-no under the securities laws. Is the SEC investigating Equifax? Given the appearance of insider trading, it is quite likely. Will the Equifax issue put more scrutiny on the work registrants are doing to protect from cyberattacks? Most certainly. In the wake of the Equifax breach and the SEC's own humiliating data breach, it is time for SEC registrants (and other companies with an internet presence and a general concern for business continuity) to consider taking a closer look at their cybersecurity measures. This is particularly true given that both Equifax and the SEC had been at risk for months before the breach was identified. And, now, if for no other reason than to deflect from its own troubles, the SEC is most certainly watching.