THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 50 No. 17 October 11, 2017

CYBERSECURITY BREACHES: AVOIDING PITFALLS

Responding to growing cyber threats, the SEC has issued regulations requiring financial firms to adopt written programs to safeguard customer records and information, and to prevent identity theft. It has also brought enforcement actions against financial firms attacked by hackers for violating the regulations. As for public companies, the SEC's principal concerns have been adequate risk disclosure and reporting of material breaches, along with sufficient internal controls. The author discusses these developments.

By Timothy D. Belevetz *

There are few issues today as important as cybersecurity. In an increasingly interconnected world, commerce and finance are dependent on rapidly evolving technology as more and more businesses operate in a cyber-driven environment. These advances have transformed commerce, making the delivery of products and services less expensive and more efficient. Yet the systems, including the most sophisticated, remain vulnerable to attacks and breaches. Hardly a day goes by without a news report about a high profile intrusion. And while a major cyber incident can have a serious impact on any business in terms of lost profits, damages, and reputational harm, regulated entities and public companies bear an additional burden — close scrutiny of the Securities and Exchange Commission.

The SEC has made it clear it expects the financial firms it regulates to institute and maintain safeguards against cyber breaches and intrusions. It also expects public companies to adequately warn investors about cybersecurity risks. Cybersecurity has had the SEC's attention for several years, and officials continue to highlight the agency's focus on the ways regulated entities and issuers are preparing for and reporting intrusions, and disclosing the risks of such attacks.

During his March 2017 confirmation hearing before the Senate, now-SEC Chairman Jay Clayton expressed his support for requirements that public companies disclose more extensive information about their cybersecurity efforts — and that the disclosure requirements should be driven by materiality. Clayton's comments were prompted by a question from Sen. Mark Warner of Virginia about whether the SEC should expand the disclosure rules related to cyber attacks. Sen. Warner had expressed concern regarding Yahoo Inc.'s disclosure in September 2016 that it had been the victim of a 2014 attack that affected 500 million users accounts. In addition, recently appointed Co-Director of the Enforcement Division, Steve Peikin, said in an interview in June that he believes "[t]he greatest threat to our markets right now is the cyber threat."[1] Co-Director

[1] Sarah N. Lynch, *Exclusive: New SEC enforcement chiefs see cyber crime as biggest market threat*, REUTERS, June 8, 2017, *avail. at* http://www.reuters.com/article/us-usa-sec-enforcement-exclusive-idUSKBN18Z2TX.

* *TIMOTHY D. BELEVETZ is a partner at Holland & Knight LLP. His e-mail address is Timothy.Belevetz@hklaw.com.*