Inside the SEC's Statement on Cybersecurity

By **Douglas Chia** October 1, 2017

I strongly urge everyone to read SEC Chair Jay Clayton's recent Statement on Cybersecurity. One part of the statement is receiving a lot of attention. Last month, the Commission learned that an incident previously detected in 2016 may have provided the basis for illicit gain through trading. While the Commission believes the intrusion (the exploitation of a software vulnerability in the test filing component of the EDGAR system) did not result in unauthorized access to personally identifiable information, jeopardize its operations, or result in systemic risk, it openly admits that it did result in access to nonpublic information of issuers. The statement did not say whether any of the issuers' nonpublic information that was exposed was material, and there's no way it could possibly determine that. The Commission's investigation of this matter is ongoing.

This statement by Chair Clayton is extraordinary and will have critics questioning the Commission's own credibility when it beseeches issuers to beef up their cybersecurity systems and disclosures. However, the statement also raises some important questions:

1. **Should the language disclosing the EDGAR breach have been in the title or first paragraph of the statement, and should the Commission have disclosed the breach immediately upon discovering it in August instead of waiting until September?** One could easily imagine those questions appearing in a comment letter from the Commission's Division of Corporation Finance staff in a review of an

issuer's 1934 Act disclosures with a similar fact pattern. How would investors or the Commission's staff react if an issuer's press release or SEC filing about cybersecurity did not mention an actual breach until 1,400 words into it, in the 17th paragraph? And, as far as timing goes, should the EDGAR breach have been disclosed earlier, say within four business days of discovery? Cue to the old Senator Howard Baker Watergate hearings question, "What did [they] know and when did [they] know it?"

2. **How might the Commission's recent experience with its own cybersecurity inform its future enforcement actions and disclosure reviews?** Critics often complain that the Commission's staff doesn't understand the challenges and complexities of the companies it regulates and as a result doesn't get its enforcement actions or disclosure comments right. While this isn't really an "eat your own cooking" or "pot calling the kettle black" moment, it may be a "teachable" moment for the Commission and its staff as they carry out their responsibilities going forward. Chair Clayton states, "I recognize that even the most diligent cybersecurity efforts will not address all cyber risks that enterprises face. That stark reality makes adequate disclosure no less important. Malicious attacks and intrusion efforts are continuous and evolving, and in certain cases they have been successful at the most robust institutions and at the SEC itself." Still, he goes on to state, "[u]ltimately, a large portion of the costs incurred in connection with these risks, including the costs of mitigation, are borne by investors, consumers, and other important constituents," reminding us that the Commission's mission is first and foremost to protect investors, not companies, boards, or management. So, companies should not expect much, if any, additional empathy from the attorneys at the Commission's Division of Enforcement, even after this event.
3. **How will this impact the debate over cyber expertise on public company boards of directors?**Corporate stakeholders—most notably investors, cyber experts, and Congress—have been urging boards to ensure at least some of their directors have legitimate cybersecurity expertise. The Equifax hacking debacle is only the most recent in a long line of incidents that have prompted calls to action. Recall the bipartisan bill in Congress that (if signed into law and adopted by the Commission) could effectively mandate every board to have a member who is a *bona fide*cybersecurity expert, similar to the Sarbanes-Oxley Act's requirement that every

board have an "audit committee financial expert." And, while the primary aim of the recently-announced next phase of the New York City Comptroller's Boardroom Accountability Project campaign is to "ratchet up the pressure on some of the biggest companies in the world to make their boards more diverse, independent, and climate-competent," the director skills matrix that the Comptroller has asked companies (151 so far) to provide to him and disclose to all investors could eventually be used to highlight a board's cybersecurity expertise or lack thereof. The samplematrix the Comptroller provides on its website includes categories called "Risk Management" and "Technology/Systems." It's probably just a matter of time before those categories spawn a "Cybersecurity" or "Information Security" box to check in some company's proxy statement, which could mark the beginning of a real trend.