The SEC Gets Hacked: What Now?

10.09.2017 | By James H. Vorhis

It was recently revealed that the Securities and Exchange Commission's ("SEC") EDGAR database, which is used by public companies to file official documents, was breached. According to the SEC, trading off of that hacked information may have reaped millions of dollars for the hackers. While discovering a hack is always startling for a private company, it is downright embarrassing for a government agency that purports to monitor cybersecurity. As a result, the hack may have long-term impacts on the SEC's role as a cybersecurity regulator and any litigation it may bring on this topic.

We have recently blogged about statements made by officials at the SEC concerning its plans to police this area. The statements have been somewhat inconsistent. At times, the SEC has indicated that they would be bringing enforcement actions against public companies for failures to make accurate cybersecurity disclosures. Other times, officials have indicated they would take a more hands-off, company-friendly approach.

How will the SEC respond in the wake of its own data breach? Currently, there remains a mishmash of rules and regulations governing cybersecurity and data breaches, and a void on who is leading the enforcement charge. No federal regulator has yet stepped forward to firmly take the reins, although the Federal Communications Commission has filed some litigation, and at least one court has granted the Federal Trade Commission regulatory power to impose liability on companies who fail to implement reasonable security measures. In light of the current breach, the SEC could be gun shy about taking the lead. However, in time, we expect that the SEC will use this breach as the impetus for playing a bigger role, i.e., claiming that it understands this area better than any other public agency. As any target of an SEC investigation can attest, the SEC feels strongly about its cybersecurity mission.

But, and it is a big but, the SEC's credibility has undoubtedly been undermined by this breach, which may impact the SEC's ability to pursue defendants going forward. Targeted defendants may point to the SEC's own data breach to bolster its defense. What better guiding point to set the standard of care in this area than the SEC itself. Usually, one of the most difficult aspects of litigating against a government agency is

putting that agency on trial. However, that problem decreases significantly when the government agency sues someone for the exact same wrong that it itself suffered. Expect interesting evidentiary and discovery challenges as parties try to attack the SEC with this breach.