Articles + Publications | October 17, 2018

Cyber Threats and Internal Accounting Controls

WRITTEN BY

Shannon Kelly

On October 16, 2018, the Securities and Exchange Commission ("SEC") issued an investigative report (see here) pursuant to Section 21(a) of the Securities Exchange Act of 1934 (the "Exchange Act") warning public companies that become victims of cyber-related frauds that they may violate the federal securities laws if they fail to have a sufficient system of internal accounting controls. Under the Exchange Act, public companies are required to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed with, or that access to company assets is permitted only with, management's general or specific authorization.

As detailed in the report, the SEC's Division of Enforcement investigated nine public companies that fell victim to cyber fraud resulting in millions of dollars of losses, most of which was not recovered. The SEC's investigations focused on "business email compromises" ("BECs") in which cyber criminals posed as company executives or vendors and used emails to dupe company personnel into sending money to bank accounts controlled by the criminals. In some cases, the frauds lasted for months and were only detected by third parties, including law enforcement. The FBI estimates that BECs have caused over $5 billion in losses since 2013. Although the SEC determined not to pursue any enforcement action against the investigated companies, it issued the report in the public interest to ensure public companies and other market participants are aware that spoofed or manipulated emails are a serious problem and should be taken into account when devising and maintaining a system of internal accounting controls.

While most of the media attention regarding cyberattacks focuses on stolen customer data, this is a timely reminder that a public company's tangible assets, including cash, are a target for cyber criminals. As noted by SEC Chairman Jay Clayton, "Cyber frauds are a pervasive, significant, and growing threat to all companies, including our public companies. Investors rely on our public issuers to put in place, monitor, and update internal accounting controls that appropriately address these threats."

RELATED INDUSTRIES + PRACTICES

- Capital Markets

©2026 Troutman Pepper Locke