Press Release

SEC Investigative Report: Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls

FOR IMMEDIATE RELEASE
2018-236

Washington D.C., Oct. 16, 2018 — The Securities and Exchange Commission today issued an investigative report cautioning that public companies should consider cyber threats when implementing internal accounting controls. The report is based on the SEC Enforcement Division's investigations of nine public companies that fell victim to cyber fraud, losing millions of dollars in the process.

The SEC's investigations focused on "business email compromises" (BECs) in which perpetrators posed as company executives or vendors and used emails to dupe company personnel into sending large sums to bank accounts controlled by the perpetrators. The frauds in some instances lasted months and often were detected only after intervention by law enforcement or other third parties. Each of the companies lost at least $1 million, two lost more than $30 million, and one lost more than $45 million. In total, the nine companies wired nearly $100 million as a result of the frauds, most of which was unrecoverable. No charges were brought against the companies or their personnel.

The companies, which each had securities listed on a national stock exchange, covered a range of sectors including technology, machinery, real estate, energy, financial, and consumer goods. Public issuers subject to the internal accounting controls requirements of Section 13(b)(2)(B) of the Securities Exchange Act of 1934 must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly. The FBI estimates fraud involving BECs has cost companies more than $5 billion since 2013.

"Cyber frauds are a pervasive, significant, and growing threat to all companies, including our public companies," said SEC Chairman Jay Clayton. "Investors rely on our public issuers to put in place, monitor, and update internal accounting controls that appropriately address these threats."

Stephanie Avakian, Co-Director of the SEC Enforcement Division, said, "In light of the facts and circumstances, we did not charge the nine companies we investigated, but our report emphasizes that all public companies have obligations to maintain sufficient internal accounting controls and should consider cyber threats when fulfilling those obligations."

The issuance of the SEC's report coincides with National Cybersecurity Awareness Month.

In consultation with the Division of Corporation Finance and the Office of the Chief Accountant, the SEC's investigations were conducted by Brent Wilner, Creighton Papier, and Maria Rodriguez, and supervised by Diana Tani, John Berry, and Michele Layne of the Los Angeles Regional Office.

###

Related Materials

- Report of Investigation