Securities Regulation Daily Wrap Up, SEC NEWS AND SPEECHES—SEC: Deficient internal controls led to cyber frauds that spoofed executives and vendor, (Oct. 16, 2018)

Securities Regulation Daily

Click to open document in a browser

By Amanda Maine, J.D.

The SEC has issued a report warning that public companies should consider cyber threats in their internal accounting controls. The report states that nine issuers, which the report did not name, were victims of schemes involving spoofed or compromised electronic communications from persons claiming to be executives of the companies or their vendors.

Business email compromises. According to the SEC, these "business email compromises" (BECs) used emails to dupe employees at these companies into sending millions of dollars of company funds to bank accounts controlled by the perpetrators of the schemes. The nine companies described in the SEC report lost at least $1 million each due to these schemes. One company lost more than $45 million, and two companies lost more than $30 million, the report states. Most of the funds lost were unrecoverable.

The SEC's report stated that the schemes employed by the fraudsters entailed emails from fake executives where the email domain appeared to be legitimate. The so-called executives directed company finance employees to work with an outside attorney to make large wire transfers to foreign bank accounts, which were controlled by the perpetrators.

The SEC also described emails from fake vendors impersonating the companies' actual vendors. According to the SEC, this scam was more "technologically sophisticated" than the fake executive emails. The vendor scheme, instead of using spoofed executive accounts, involved the fraudsters hacking the existing vendors' email accounts and inserting illegitimate requests for payments and payment processing details. The perpetrators would use this information to request changes to the vendors' banking information and would then attach invoices reflecting new and fraudulent account information. As a result, issuers made payments on these fake invoices to foreign accounts controlled by the fraudsters, according to the SEC.

Internal controls. The SEC is not bringing charges against the companies or the personnel that were targeted by the scheme. However, the report emphasizes that companies must devise and maintain a system of internal accounting controls that are attuned to these kinds of frauds. According to the report, the issuers did have systems in place to verify authorization of payment request, as well as management approval for outgoing wires and verification of changes to vendor data. These controls were not enough to protect the issuers from being victimized by the fraudsters, the SEC warned.

Internal accounting controls must be reassessed in light of emerging cyber-related risks, the SEC advised. While the SEC is not charging the companies described in the report, Enforcement Co-Director Stephanie Avakian reiterated that "all public companies have obligations to maintain sufficient internal accounting controls and should consider cyber threats when fulfilling those obligations."

RegulatoryActivity: Enforcement FraudManipulation SECNewsSpeeches