Published on *The National Law Review* https://natlawreview.com

SEC's latest Cyber-Fraud ROI Indicates Future Enforcement Against Hacker Victims . . . Fool Me Twice

Article By:

Bill Mateja

Sarah E. Aberg

Jennifer N. Le

In the aftermath of the Securities and Exchange Commission's ("SEC") latest Report of Investigation ("Report") regarding cyberattacks via "spoofed or manipulated electronic communications," companies should prepare to adjust and update their internal controls or face possible enforcement actions for violation of federal securities law. Released as a warning to public companies about recent cyberattacks, the Report's emphasis that companies maintain proper internal controls to combat cybersecurity issues indicates SEC enforcement actions for lack of proper cybersecurity procedures and supervision are on the horizon.

The Report, released on October 16, revealed the SEC's investigation into nine public companies that fell victim to cyber-related frauds, leading to a combined loss of over $100 million. The frauds entailed employees wiring large sums or paying invoices to fake accounts after receiving "spoofed" or "compromised electronic communications" purporting to be from company executives, lawyers, or vendors. The fake emails from executives employed unsophisticated technology requiring only the creation of email addresses that mimicked the look and design of an executive's actual email address. These emails all had common themes, which included: poor grammar, secrecy, time urgent transactions, suggestion of government oversight, and a need to transact business in foreign countries. The fake vendor emails were more insidious and involved the hacking of email accounts of legitimate foreign vendors working with the companies. These emails contained fewer hints of illegitimacy or red flags, and thus, many of the victimized companies only learned of the fraud after actual vendors raised concerns about outstanding invoices. The SEC did not name the companies involved, but did note that the cyber-related frauds affected companies from various industries—demonstrating that all companies are potentially at risk.

The SEC's investigation assessed whether these companies had sufficient controls to guard against the cyberattacks and thus "provide reasonable assurances that transactions are executed with, or that access to company assets is permitted only with, management's general or specific authorization" pursuant to the requirements of Sections 13(b)(2)(B)(i) and (iii) of the Securities

Exchange Act of 1934 (the “1934 Act”). Notably, the SEC did not pursue enforcement actions against any of the nine companies.

Instead, the SEC issued the Report to highlight the 1934 Act’s requirement that companies must implement sufficient internal procedures and controls to prevent unauthorized access to company assets – which means companies must have adequate controls to identify and prevent cyberattacks such as the ones identified in the Report. The Report acknowledged that cyber-related threats are a new facet of today’s world, but noted the expectations that companies maintain proper internal controls that adjust to changing circumstances are not. The Report also underscored the importance of creating specially designed controls that targeted cyber-related fraud, including providing critical trainings to employees to help them recognize signs of cyber-fraud, and ensure employees follow proper protocols for payment authorization.

The Report is a clear warning that cybersecurity issues are front and center at the SEC and that companies must implement proper controls to prevent cyber-related fraud. As cybersecurity remains a focus for the SEC, companies should work with their attorneys and IT and compliance personnel to establish procedures to combat ever-changing cyber threats. Companies unwilling to do this risk not only potential hacks and frauds, but also enforcement liability under the securities laws.

National Law Review, Volume VIII, Number 332