Linklaters

October 2018

U.S. Securities Law Briefing:
SEC Warns Public Companies to Reassess Internal Accounting Controls in Light of Cyber Scams

In another reminder that public companies must take cybersecurity seriously, the U.S. Securities and Exchange Commission (the "SEC") recently issued a Report of Investigation (the "Report") warning companies to consider whether their internal accounting control systems are sufficient to provide reasonable assurances in safeguarding their assets from cyber threats.

The Report, which is based on the SEC Enforcement Division's investigations of nine public companies that were victims of cyber fraud, follows the SEC's release earlier this year of interpretive guidance on cybersecurity disclosures as well as its first cybersecurity disclosure enforcement action.

Although the Enforcement Division chose not to pursue enforcement actions in these nine cases, the SEC cautioned that public companies should pay particular attention to the obligations imposed by Section 13(b)(2)(B) of the U.S. Securities Exchange Act of 1934 (the "Exchange Act"), which requires issuers to devise and maintain internal accounting controls that reasonably safeguard company and, ultimately, investor assets from cyber-related frauds. The provision requires issuers to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed in accordance with management's general or specific authorization," and that "access to assets is permitted only in accordance with management's general or specific authorization."

The cases primarily involved emails from fake executives and fake vendors, resulting in a total loss of nearly $100 million from nine companies, with each company losing at least $1 million and two losing more than $30 million. The Report notes that the "frauds were not sophisticated in design or the use of technology; instead, they relied on technology to search for both weaknesses in policies and procedures and human vulnerabilities that rendered the control environment ineffective." Therefore, the Report says, having internal accounting control systems that factor in such cyber-related threats, and related human vulnerabilities, is important.

Although the Report does not direct issuers to adopt any specific controls, it does highlight the "critical role" of training in implementing controls. Many of the frauds succeeded, at least in part, because the responsible personnel did not sufficiently understand existing controls or did not recognize indications that the emails lacked reliability. And in many cases, the recipients of the fraudulent emails asked no questions about the nature of the supposed

transactions, even where such transactions were clearly outside of the recipient employee's domain, and where the employee was asked to make multiple payments over days and even weeks.

* * * * *

Although the Report states that not every issuer that is a victim of a cyber scam is in violation of the internal accounting controls requirements of the federal securities laws, it makes clear that many issuers should be reassessing their internal accounting controls in light of the prevalence and continued expansion of cyber-related frauds.

Training should be a particular area of focus. Most of the issuers that were the subject of the Report had some form of training regarding controls and information technology in place prior to the scams. After the incidents, all of them enhanced their training of responsible personnel about relevant threats, as well as about pertinent policies and procedures.

We will continue to monitor developments in this area and welcome any queries you may have. We would be happy to discuss with companies their internal accounting control systems in conjunction with our Technology, Media and Telecommunications and Operational Intelligence Groups.

Contacts

For further information, please contact:

Mike Bienenfeld
Partner

+44 20 7456 3660

mike.bienenfeld@linklaters.com

Jeffrey Cohen
Partner

+1 212 903 9014

jeffrey.cohen@linklaters.com

Doug Davison
Partner

+1 202 654 9244

doug.davison@linklaters.com

Matthew Poulter
Partner

+1 212 903 9306

matthew.poulter@linklaters.com

Luis Roth
Partner

+33 1 56 43 58 42

luis.roth@linklaters.com

Pam Shores
Partner

+44 20 7456 4650

pam.shores@linklaters.com

Tom Shropshire
Partner

+44 20 7456 3223

tom.shropshire@linklaters.com

or any of your other usual Linklaters contacts.

Linklaters.com