October 24, 2018

Implementing Internal Controls in Cyberspace – Old Wine, New Skins

On October 16, 2018, the SEC issued a Section 21(a) investigative report (the "Report"),[1] cautioning public companies to consider cyber threats when designing and implementing internal accounting controls. The Report arose out of an investigation focused on the internal accounting controls of nine public companies that were victims of "business email compromises" 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. In the investigation, the SEC considered whether the companies had complied with the internal accounting controls provisions of the federal securities laws. Although the Report is in lieu of an enforcement action against any of the issuers, the SEC issued the Report to draw attention to the prevalence of these cyber-related scams and as a reminder that all public companies should consider cyber-related threats when devising and maintaining a system of internal accounting controls.

The nine defrauded companies lost a total of nearly $100 million as a result of the email scams. The companies operated in different business sectors including technology, machinery, real estate, energy, financial, and consumer goods, which the Report suggests "reflect[s] the reality that every type of business is a potential target of cyber-related fraud." The Report also highlighted the significant economic harm posed by "business email compromises" more broadly, which, based on FBI estimates, has caused over $5 billion in losses since 2013, with an additional $675 million in adjusted losses in 2017—the highest estimated out-of-pocket losses from any class of cyber-facilitated crime during this period.

Two types of email scams were employed against the nine companies: (i) emails from fake executives, and (ii) emails from fake vendors.

Emails from Fake Executives. In the first type of scam, perpetrators emailed company finance personnel using spoofed email domains and addresses of an executive (typically the CEO) so that it appeared as if the email were legitimate. The spoofed email directed the employees to work with a purported outside attorney identified in the email, who then directed them to wire large payments to foreign bank accounts controlled by the perpetrators. Common elements among each of these schemes included: (1) the transactions or "deals" were time-sensitive and confidential; (2) the requested funds needed to be sent to foreign banks and beneficiaries in connection with foreign deals or acquisitions; and (3) the spoofed emails typically were sent to midlevel personnel, who were not generally responsible or involved in the deals and rarely communicated with the executives being spoofed.

Emails from Fake Vendors. The second type of scam was more technologically sophisticated than the spoofed executive emails because the schemes typically involved the perpetrators hacking into the email accounts of the companies' foreign vendors. The perpetrators then requested that the vendors' banking information be changed so that a company's payments on outstanding invoices for legitimate transactions were sent to foreign accounts controlled by the perpetrators rather than the real vendors. The Report noted that some spoofed vendor email scams went undetected for an extended period of time because vendors often afforded companies months before considering a payment delinquent.

Considerations for Public Companies

In the Report, the SEC advises public companies to "pay particular attention to the obligations imposed by Section 13(b)(2)(B) to devise and maintain internal accounting controls that reasonably safeguard company and, ultimately,

[1] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements, Exchange Act Release No. 84429 (Oct. 16, 2018) (available here).

investor assets from cyber-related frauds." Finance and accounting personnel at public companies should be aware that the above-described cyber-related scams exist, and these types of scams should be considered when implementing internal accounting controls.

Although the "cyber" aspect of these scams helps to make them a topic *du jour*, fake invoices are certainly no recent invention, nor are vendor requests to direct payments to a new address something that is unique to the email era. If the result of the Report is to cause companies to liberally insert "cyber" references into their internal controls, and little more, it will not have accomplished its objective. SEC Enforcement staff observed that the cyber-related frauds succeeded, at least in part, because the responsible personnel at the companies did not sufficiently understand the company's **existing** controls or did not recognize indications in the emailed instructions that those communications lacked reliability. For example, in one matter, the accounting employee who received the spoofed email did not follow the company's dual-authorization requirement for wire payments, directing unqualified subordinates to sign-off on the wires. In another case, the accounting employee misinterpreted the company's authorization matrix as giving him approval authority at a level reserved for the CFO.

Scams will always be with us, and the Report recognizes that the effectiveness of internal accounting control systems largely depends on having trained personnel to implement, maintain, and follow such controls. Public companies should also consider the following points raised by the actions taken by the defrauded companies following the cyber-related scams:

- Review and enhance payment authorization procedures, verification requirements for vendor information changes, account reconciliation procedures and outgoing payment notification processes, particularly to foreign jurisdictions.

- Evaluate whether finance and accounting personnel are adequately trained on relevant cyber-related threats and provide additional training on any new policies and procedures implemented as a result of the above step.

The Report confirms that the SEC remains focused on cybersecurity matters and companies should continue to be vigilant against cyber threats. While the SEC stated that it was "not suggesting that every issuer that is the victim of a cyber-related scam is . . . in violation of the internal accounting controls requirements of the federal securities laws," the Report also noted that "[h]aving internal accounting control systems that factor in such cyber-related threats, and related human vulnerabilities, may be vital to maintaining a sufficient accounting control environment and safeguarding assets."

Please feel free to contact any member of Ropes & Gray's securities & public companies or privacy & cybersecurity practice groups with any questions about this Alert.