SEC Investigative Report on Cybersecurity Emphasizes Internal Controls

Skadden

10 / 19 / 18

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

Four Times Square
New York, NY 10036
212.735.3000

1440 New York Ave., N.W.
Washington, D.C. 20005
202.371.7000

On October 16, 2018, the Securities and Exchange Commission (SEC) issued a Report of Investigation (Report) detailing an investigation by the SEC's Enforcement Division into the internal accounting controls of nine issuers that were victims of "business email compromises," a form of cyberfraud.[1] The SEC issued the Report pursuant to Section 21(a) of the Securities Exchange Act, forgoing a traditional enforcement action, to communicate the SEC's view that this issue is problematic and to put issuers and individuals on notice that the SEC intends to pursue enforcement actions concerning similar conduct in the future.

In the Report, the SEC cautioned issuers that they should consider cyberthreats when implementing internal accounting controls. This follows recent SEC guidance[2] and an enforcement action highlighting the need for prompt disclosure of data breaches and other cybersecurity incidents as well as the creation of the Cyber Unit, a unit within the SEC's Enforcement Division focused on targeting cyber-related misconduct. In releasing the Report, the SEC is sending a clear message that it expects issuers to not only act responsibly in the event of a cybersecurity incident but also to institute appropriate controls to mitigate the risks of cyber-related threats and safeguard company assets from those risks.

Key Takeaways

- As "every type of business is a potential target of cyber-related fraud," according to the Report, every issuer, regardless of sophistication or size, should prioritize cybersecurity.
- Issuers are expected to evaluate the cybersecurity risks facing their particular business models and implement internal controls tailored to address those risks.
- After implementation, issuers should continually assess the cybersecurity risks they face and calibrate their internal controls accordingly.
- Issuers should maintain policies and procedures that ensure relevant information regarding cybersecurity risks and incidents is collected, processed and escalated on a timely basis, and issuers should prioritize the training of employees on those policies and procedures.
- In disclosing cybersecurity risks and incidents, issuers should avoid boilerplate language and tailor disclosures to their specific business and industry.
- Issuers should consider whether their insider trading policies are designed to prevent trading on material nonpublic information related to cybersecurity risks and incidents.

Investigative Report

The SEC's investigation concerned whether nine issuers complied with federal securities laws, including Section 13(b)(2)(B) of the Exchange Act, by designing and maintaining internal accounting controls that reasonably safeguarded the issuers from cyber-related risks. Section 13(b)(2)(B) requires certain issuers to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that," among other things, "transactions are executed in accordance with management's general or

[1] "Report of Investigation Pursuant to 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements," SEC Release No. 34-84429 (Oct. 16, 2018).

[2] See our February 23, 2018, client alert, "SEC Issues Interpretive Guidance on Cybersecurity Disclosures."

SEC Investigative Report on Cybersecurity Emphasizes Internal Controls

specific authorization" and "access to assets is permitted only in accordance with management's general or specific authorization." The issuers described in the Report lost a combined $100 million after their internal accounting controls failed to protect against two types of fraudulent email schemes.

In the first type of scheme, a person not affiliated with an issuer allegedly sent an email to a finance employee at an issuer using a spoofed email domain and address — which mimicked the email account of one of the issuer's executives — directing the employee to wire funds in connection with a certain transaction. The email allegedly directed the employee to work with a purported outside attorney, who then asked the employee to transfer the funds to a foreign bank account controlled by the alleged perpetrators. The SEC noted that this type of fraud is unsophisticated from a technological standpoint — it requires only the creation of an email address that seemingly belongs to an executive of an issuer.

The second more technologically complex type of fraudulent scheme is one in which the alleged perpetrators hacked the email accounts of issuers' foreign vendors and sent payment requests to employees at the issuers for services rendered. The alleged perpetrators provided the employees with revised banking information and wire instructions that were linked to foreign accounts that the perpetrators controlled. Issuer employees allegedly transferred funds to the foreign accounts, only discovering the fraud months later when the actual vendors sought payment on their outstanding invoices.

The Report highlights the need for issuers to design and maintain internal accounting control systems that adequately address the cybersecurity risks they face. The persons undertaking the alleged cyber-related frauds were able to identify vulnerabilities in the issuers' controls over, for instance, payment authorization and verification procedures. Issuers need to ensure that their internal accounting controls are tailored to address, among other things, human vulnerabilities with respect to cyber-related risks. The Report explains that the alleged perpetrators succeeded in the frauds in large part because employees were unaware of, or did not understand, the internal controls of their employers and failed to recognize multiple red flags indicating that a fraudulent scheme was underway.

The SEC's Heightened Interest in Cybersecurity

The Report comes just over a year after the SEC announced the creation of its Cyber Unit in September 2017.[3] The Cyber Unit was formed to consolidate the expertise of the SEC's Division of Enforcement and enhance its ability to identify and investigate cyber-related threats. In commenting on the Cyber Unit's launch, Stephanie Avakian, co-director of the SEC's Enforcement Division, identified cyber-related threats as "among the greatest risks facing investors and the securities industry."

The Cyber Unit complements the cybersecurity working group, an initiative of SEC Chairman Jay Clayton, to coordinate information sharing, risk monitoring and incident response throughout the SEC. In establishing the working group, Chairman Clayton announced the SEC's focus "on identifying and managing cybersecurity risks and ensuring that market participants — including issuers, intermediaries, investors and government authorities — are actively engaged in this effort and are appropriately informing investors and other market participants of these risks."[4]

In April 2018, the Cyber Unit was involved in bringing a cyber-related enforcement action against a technology company for allegedly misleading shareholders by not disclosing a data breach in its public filings for nearly two years.[5] The $35 million settlement was the first SEC enforcement action against a public company relating to the disclosure of a data breach. According to the SEC, the company failed to establish or implement internal controls around the evaluation and disclosure of cyber incidents. The SEC alleged that the company's senior management and legal staff "did not properly assess the scope, business impact, or legal implications of the breach, including how and where the breach should have been disclosed in [its] public filings or whether the breach rendered, or would render, any statements made by [it] in its public filings misleading."

[3] "SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors," SEC Press Release No. 2017-176 (Sept. 25, 2017).

[4] "Statement on Cybersecurity," SEC Chairman Jay Clayton (Sept. 20, 2017).

[5] "Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cyber Security Breach; Agrees to Pay $35 Million," SEC Press Release No. 2018-71 (Apr. 24, 2018).

SEC Investigative Report on Cybersecurity Emphasizes Internal Controls

The SEC noted that the company's disclosures in its public filings were misleading to the extent they omitted known trends or uncertainties presented by the data breach. In addition, the SEC alleged the risk factor disclosures in the company's public filings were misleading in that they claimed the company only faced the risk of potential future data breaches without disclosing that a data breach had in fact already occurred. The SEC noted that while immediate disclosure (such as in a Form 8-K) is not always necessary in the event of a data breach, in this case, the breach should have been disclosed in the company's regular periodic reports.

Prior Interpretive Guidance

In February 2018, the SEC issued interpretative guidance regarding disclosures concerning cybersecurity risks and incidents.[6] The SEC's guidance provides that, in disclosing cybersecurity risks and incidents, issuers should avoid boilerplate language and tailor disclosures to their specific businesses and industries, including disclosing the potential financial, legal or reputational impacts of cybersecurity risks or incidents. The disclosures should not be so detailed, however, that they compromise companies' cybersecurity efforts.

The guidance also advises issuers to evaluate their cybersecurity policies and procedures, and ensure that relevant information pertaining to cybersecurity risks and incidents is collected, processed and escalated on a timely basis so management can assess and analyze whether disclosure is required. The guidance encourages issuers to evaluate whether their insider trading policies are designed to prevent insider trading on the basis of material nonpublic information relating to cybersecurity incidents and risks. The guidance notes that issuers should consider restrictions on trading during periods when issuers are investigating and assessing the significance of a cybersecurity incident.

[6] "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," SEC Release Nos. 33-10459; 34-82746 (Feb. 26, 2018).

SEC Investigative Report on Cybersecurity Emphasizes Internal Controls

Securities Enforcement

Andrew M. Lawrence
Partner / Washington, D.C.
202.371.7097
andrew.lawrence@skadden.com

Colleen P. Mahoney
Partner / Washington, D.C.
202.371.7900
colleen.mahoney@skadden.com

Charles F. Walker
Partner / Washington, D.C.
202.371.7862
charles.walker@skadden.com

Joshua A. Ellis
Counsel / Washington, D.C.
202.371.7724
joshua.ellis@skadden.com

SEC Reporting and Compliance

Brian V. Breheny
Partner / Washington, D.C.
202.371.7180
brian.breheny@skadden.com

Caroline S. Kim
Associate / Washington, D.C.
202.371.7555
caroline.kim@skadden.com

Cybersecurity and Privacy

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

Associate **Sydney P. Sgambato** assisted in the preparation of this alert.