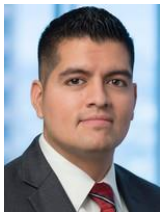
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New SEC Cyber Report Puts Spotlight On Accounting Controls

By **George Garvey, Grant Davis-Denny, Nefi Acosta and Najee Thornton**
(October 23, 2018, 1:28 PM EDT)

George Garvey

Grant Davis-Denny



Nefi Acosta

Najee Thornton

Imagine you work as an accounts payable employee at a publicly traded company called Forevernet. Late on a Friday afternoon, as you prepare to depart for a long weekend, an email arrives from John.Thompson@forevemet.com. You know Thompson to be the chief financial officer of your company and in your haste to respond to his urgent email, you overlook the fact that the sender's email domain just barely changes the spelling of your company's actual domain, forevernet.com (substituting an "m" for an "rn"). The sender, posing as your CFO, informs you that a deal with an important foreign counterparty has been struck. He directs you to work with outside counsel, whom he has copied on the email, to make the necessary wire payment of $1.295 million before close of business. You haven't communicated with this outside attorney before. But the email domain, JonesHammmersmithllp.com, appears legitimate. So you reply all that you will be glad to facilitate the wire transfer, shortly thereafter receive wire instructions from the purported outside counsel, and promptly process the transaction.

You and your employer have fallen victim to a cyberfraud known as a business email compromise, or BEC, attack. You are not alone. According to a recent report from the FBI's Internet Crime Complaint Center, there were over 78,000 worldwide incidents of BEC scams from October 2013 to May 2018 (and over 41,000 in the United States). Victims lost approximately $12.5 billion. And the threat is on the rise. Between December 2016 and May 2018, there was a 136 percent increase in identified global exposed losses from BEC attacks.[1]

In light of a U.S. Securities and Exchange Commission report issued Oct. 16, 2018, the consequences of such an attack may extend beyond financial losses.[2] A successful attack may, in certain circumstances, now raise the risk of an SEC investigation and enforcement action.

Background on the SEC's Role in Public Company Cybersecurity

Although the SEC does not regulate the type of data security technical controls that most publicly traded companies must employ,[3] the SEC increasingly has used its regulatory authority to wade into the cybersecurity regulatory landscape.

In 2011, the SEC's Division of Corporation Finance issued guidance regarding the disclosure obligations

of publicly traded companies relating to cybersecurity risks and incidents.[4] Drawing on such companies' general obligations to disclose risks and events that a reasonable investor would consider important to an investment decision, the guidance indicated that cyber risks and incidents can, like other operational and financial risks, require disclosures to investors in certain circumstances.

Earlier this year, the SEC issued further guidance on public company cybersecurity disclosures.[5] In addition to reiterating points made in its 2011 guidance, the February 2018 guidance provided additional insight into the SEC's views on required disclosures, emphasized the importance of cybersecurity policies and procedures that allow for timely and effective disclosure, and discussed the applicability of insider trading restrictions in the event of a cybersecurity incident.

The SEC's 21(a) Report on BEC Attacks

On Oct. 16, 2018, the SEC issued a type of report, known as a "21(a) report," on BEC attacks. The report warrants careful examination. These 21(a) reports often function as a warning to public companies and their counsel that enforcement charges could be brought in similar circumstances in the future.

The SEC's BEC report is based on the Enforcement Division's investigation of nine publicly traded companies that were victims of BEC attacks. All nine lost millions of dollars through BEC attacks; two forfeited more than $30 million to cybercriminals. The SEC did not bring charges against the victims, but it used the occasion "to make issuers and other market participants aware that these cyber-related threats of spoofed or manipulated electronic communications exist and should be considered when devising and maintaining a system of internal accounting controls as required by the federal securities laws."[6]

Not Just a Matter for Disclosure

Unlike its earlier cybersecurity guidance to public issuers, the SEC's BEC report is not focused on an issuer's disclosure obligations. The SEC's reference to internal accounting controls arises from Section 13(b)(2)(B) of the Securities Exchange Act. That provision requires issuers to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances [among other things] that (i) transactions are executed in accordance with management's general or specific authorization," and that "(iii) access to assets is permitted only in accordance with management's general or specific authorization." Section 13(b)(2)(B), enacted as part of the Foreign Corrupt Practices Act, is not by its terms limited to accounting controls that have an effect on the issuer's financial reporting and other disclosures to investors. (Nor, despite its origins in the FCPA, is its language limited to situations involving foreign activity or bribery.)

The BEC report signals that the SEC might take action against issuers whose internal controls are insufficient even where the vulnerability does not render the issuers' financial reports misleading. And issuers should expect their auditors to make inquiries informed by the BEC report when they consider the issuers' internal controls.

The report states that the SEC "is not suggesting that every issuer that is the victim of a cyber-related scam is, by extension, in violation of the internal accounting controls requirements of the federal securities laws." But it cautions "that internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds. Public issuers subject to the requirements of Section 13(b)(2)(B) must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly."[7]

A key question, then, is how public issuers can appropriately tailor their internal accounting controls to mitigate the risk of financial losses and SEC enforcement actions stemming from BEC attacks.

Two Categories of BEC Attacks

A critical first step in designing appropriate accounting controls for BEC attacks is to understand the characteristics of the two types of BEC compromises discussed in the SEC's report. Appreciating how these attacks typically occur may allow companies to more effectively train employees to recognize signs of such exploits and may suggest mechanisms, such as approval or verification procedures, that could help to minimize the risk of an attack succeeding.

The first method begins with an impersonation of an internal company executive. The example we began with illustrates this type of attack. Note that the strategy does not require a sophisticated hacker's skill set. No infiltration of firewalls or the company's physical security is needed, though such an intrusion could make the fraud even more difficult to detect (because the executive's email might then come from the executive's actual email account). The attacker simply needs to register a domain name that appears similar to the victim company's real domain name and then can use web searches, online biographies and social network sites to identify the names of relevant executives and finance department employees.

The SEC's report identifies certain factors that are typically seen in these attacks. Specifically, the initial email may:

- Direct a member of the finance staff to work with outside attorneys to effectuate the wire transfers to a foreign bank or recipient.
- Convey a sense of urgency to the supposed deal and to the wire specifically.
- Indicate that there is a need to maintain secrecy regarding the deal and instruct the recipient not to discuss the transaction with other company employees.
- Suggest that the transaction is occurring with government oversight.
- Lack significant details about the supposed deal.
- Have spelling or grammatical mistakes.

Although each of these alone may have an innocent explanation, where most or all are present, it may be a red flag that the company is being targeted by a BEC attack.

A second type of BEC attack identified in the SEC's report begins with an email from someone posing as a vendor. In this version of the attack, hackers impersonated real vendors and persuaded company employees to change the vendors' banking information so that payments for legitimate vendor invoices were made to the perpetrators' accounts instead of to the vendors' accounts.

These vendor-based attacks were particularly challenging for victims to detect for at least three reasons. First, the attackers began by breaching the vendor's systems and hijacking an actual email account. Thus, a close examination of the sender's email domain would reveal no signs of fraud. Second, the

attackers posing as vendors would obtain actual purchase orders and invoices from the company's procurement personnel and then use those real documents to generate fake versions that directed payment to a new account controlled by the attacker. Third, because vendors may wait months before asking about missing invoices (which the company believed it had already paid), it was possible for these attacks to occur over a substantial period of time.

Potential Enhancements to Accounting Controls

The SEC's report suggests several ways in which companies can enhance their accounting controls, reduce the risk of a successful BEC attack, and mitigate the chance of an SEC enforcement action or investigation.

First, public issuers should ensure they have robust cybersecurity training programs in place for their employees. After all, in some instances, it may only take a single employee's mistake for the company's security to be compromised. The SEC report noted that the victim companies it investigated had strengthened their training programs in the aftermath of the thefts. Cybersecurity training programs have traditionally focused on issues such as phishing and password protection. But the SEC's report shows that cyber education should include training on the two types of BEC attacks discussed above. In particular, accounting employees should be trained on the potential red flags that may signal a BEC attack.

Training should also address policies and procedures related to payments to third parties. The SEC found in its investigation instances where accounting employees had made payments without obtaining approvals required by their companies' existing procedures. These findings indicate that strong accounting control programs should include education practices designed to teach and remind employees of important approval and verification processes.

Companies should also assess whether their current approval and verification procedures are adequate. The SEC's report does not suggest a one-size-fits-all approach to approval and verification, and the best solution will vary based on a company's circumstances. It may be reasonable to examine, however, given the threat of BEC attacks, whether executive approval for significant payments should be conveyed orally or through some other reliable channel (and not merely through a high-level executive's email requesting the payment), or require the use of code words. In the case of changes by vendors to account payment instructions, a company may want to require that its employees obtain verbal confirmation of the change by calling a phone number that the employee knows is associated with the account (e.g., not simply the phone number provided in the vendor email requesting the change).

The SEC's report indicates that detection of BEC attacks followed by prompt steps to revise internal controls can be a sign of an effective accounting control program, rather than an indication of a flawed system. Companies therefore may want to evaluate whether their systems for detecting BEC fraud are adequate. For example, public issuers may want to institute a process where significant payments to foreign recipients trigger additional review by someone knowledgeable about BEC attacks and who was uninvolved in the initial payment.

Where a BEC attack does partially or fully succeed, a company should reassess the adequacy of its accounting controls, both to lower the risk of a future successful attack and to help demonstrate compliance with Section 13(b)(2)(B).

Finally, public issuers may want to consider whether there are other current or emerging cyberthreats

that could also implicate their duty to maintain sufficient internal accounting controls. While the SEC's report focused on the BEC threat, it is possible that other technology-based crimes, such as ransomware or attempts to extort company payments to avoid disclosure of sensitive data, could also raise accounting control concerns.

George M. Garvey and Grant A. Davis-Denny are partners, and Nefi D. Acosta and Najee K. Thornton are associates, at Munger Tolles & Olson LLP.

[1] FBI Public Service Announcement, Alert No. I-071218-PSA, Business E-Mail Compromise the 12 Billion Dollar Scam (July 12, 2018) https://www.ic3.gov/media/2018/180712.aspx.

[2] Securities and Exchange Commission, Release No. 84429, 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 (Oct. 16, 2018) (hereinafter "Section 21(a) report").

[3] This article and the SEC's 21(a) report are not focused on the SEC's regulatory authority with respect to investment advisers, broker-dealers, municipal advisers, national securities exchanges, transfer agents, and certain other market participants. A number of cybersecurity-related regulations, such as Regulation S-P, Regulation SCI, and Regulation S-ID, apply to these regulated entities but do not apply to U.S. public companies generally. The SEC also has made clear that a key priority of its national examination program for such regulated entities includes cybersecurity, including "governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response." See Securities and Exchange Commission, Office of Compliance Inspections and Examinations, 2018 National Exam Program Examination Priorities at 9 (2018).

[4] Securities and Exchange Commission, Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011).

[5] Securities and Exchange Commission, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459, 34-82746 (Feb. 26, 2018).

[6] Section 21(a) report at 2.

[7] Section 21(a) report at 6.