The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No. 36 October 31, 2018

SEC ENFORCEMENT

SEC Signals That Insufficient Internal Accounting Controls May Lead to Investigation and Enforcement

By Helen Kim, *The Cybersecurity Law Report*

Nine unnamed public companies found themselves the target of an SEC investigation after they fell victim to "business email compromises," a type of cyber fraud that cost them nearly $100 million combined. While the SEC did not initiate enforcement actions against any of these companies, the resulting Report signals the Commission's intent to add another tool (in addition to the Safeguards Rule, the Red Flags Rule, disclosure rules and others) to its arsenal to pursue companies for weak cybersecurity programs – internal accounting controls violations. In this article, we review the Report's findings with insight from Davis Polk partner Avi Gesser on SEC enforcement and how to avoid BEC scams. See also "SEC Confirms Cyber Disclosure Expectations in New Guidance" (Feb. 28, 2018).

What Is a Business Email Compromise?

At first glance, the email from your CEO, jane.kelly@abcompany.com, looks legitimate. A time-sensitive deal requires the next-day wire transfer of funds to a foreign bank, and because of government regulations, the transaction must be kept under wraps. Following procedure, you initiate the wire transfer to the bank account specified in the email.

Except that you work at ABC Company, not AB Company.

In business email compromises (BEC), cybercriminals target employees who have access to company finances and trick them into making wire transfers to bank accounts thought to belong to trusted partners. According to the FBI, perpetrators of BEC often gain access to a company's network using spear-phishing and malware, and spend weeks or months studying the company's vendors, billing systems, and the CEO's style of email communication. The scammers send an email from the CEO to a targeted employee with a request for an immediate transfer, usually to a trusted vendor, but to an account that is controlled by the criminals. Since 2013, BEC scams have caused over $5 billion in losses, according to the FBI's 2017 Internet Crime Report.

SEC's Warning to Companies With Weak Cybersecurity

The SEC recently concluded an investigation of nine public companies that were victims of one of two kinds of BEC schemes involving spoofed or compromised electronic communications. The agency did not pursue enforcement actions against these companies, but the investigation and the resulting Report of Investigation (Report), released on October 16, 2018, serve as a warning to companies that insufficient internal accounting controls may not only lead to costly cyber incidents, but also to regulatory action.

"The SEC, like other regulators, has been reluctant to come down too hard on companies in cyber cases because those companies are often victims of criminal conduct that has already caused them significant damage," said Avi Gesser, a Davis Polk partner and principal member of the firm's cybersecurity and data privacy practice.

But the Commission appears to be changing its approach. In September 2018, the SEC announced a $1-million settlement with broker-dealer and investment adviser Voya Financial Advisors Inc., for failures in cybersecurity policies and procedures related to a cyber intrusion that compromised personal information of thousands of the company's customers. "I think the message is that the SEC is really starting to bring enforcement actions against companies that have weak cybersecurity," Gesser said. "The Report itself may be more 'carrot,' but the SEC is clearly signaling that companies should expect more 'stick'" when it comes to cybersecurity.

See "Lessons From the SEC's First Red Flags Rule Settlement" (Oct. 10, 2018).

SEC Investigation and Report

The SEC's investigation considered whether nine public companies that had fallen victim to BEC scams had complied with Sections 13(b)(2)(B)(i) and (iii) of the Securities Exchange Act, which require issuers to "devise and maintain a system of internal accounting controls sufficient to provide reasonable

assurances that (i) transactions are executed in accordance with the management's general or specific authorization," and that "(iii) access to assets is permitted only in accordance with the management's general or specific authorization." While the SEC decided not to pursue any enforcement actions with regard to these nine companies, the Commission's Report described the scams and encouraged companies to maintain sufficient internal accounting controls.

Two Types of BECs

The nine companies investigated by the SEC fell victim to two types of BECs. In the first variant, the perpetrators emailed company finance personnel, using spoofed email domains and addresses, usually of the CEO, and directed the target to work with an outside attorney, who then instructed the target to wire funds to foreign bank accounts. According to the Report, these were not sophisticated frauds; the only technological aspect was creating an email address that mimicked the CEO's address. The emails described time-sensitive transactions that required secrecy, and directed funds to foreign banks and beneficiaries that would have been unusual for the company. The recipients of the emails were mid-level personnel who rarely communicated with the executives being spoofed.

In the second, more technologically sophisticated variant, the perpetrators hacked into email accounts of vendors working with the public company and inserted payment requests into emails for otherwise legitimate transactions. The perpetrators then sent doctored invoices with new, fraudulent account information, and requested the target change the bank account information to which they sent payment. Unlike the fake executive emails, the spoofed vendor emails had fewer red flags, and several victims learned of the scam only when the real vendor raised concerns about nonpayment on actual invoices.

The nine public companies that fell victim to these scams lost a total of nearly $100 million to the perpetrators. One company made 14 wire payment over several weeks resulting in over $45 million in losses, before a foreign bank alerted them about the issue. Each company lost at least $1 million.

See also "Multimillion-Dollar Scheme Serves As Backdrop for Lessons on Preventing and Mitigating Phishing Attacks" (Apr. 5, 2017).

Weaknesses in Policies and Employees' Failure to Understand Controls

The SEC noted that these scams were successful "at least in part, because the responsible personnel did not sufficiently understand the company's existing controls or did not recognize indications in the emailed instructions that those communications lacked reliability." In one case, the employee did not follow the company's dual-authorization requirement for wire payments. In another, the employee thought he had the proper approval authority, which was actually reserved for the CEO. In numerous cases, the Report stated, the recipients "asked no questions," even when the transactions were "clearly outside the recipient employee's domain." In two instances, the employees who made the wire transfers out to the fake accounts were chief accounting officers.

Gesser was not surprised that executive-level staff had fallen for the same scam as midlevel employees. "Many of these BEC scams are pretty sophisticated and take advantage of the rapid-fire decision making that is common for executives," he explained. "Unless executives are supported by strong policies, controls and training, they are just as likely, if not more likely, to miss the clues (assuming there are any clues to catch)."

The Report noted that the cyber criminals had relied on technology to search for "weaknesses in policies and procedures and human vulnerabilities that rendered the control environment ineffective." Each of the nine companies had procedures that required certain levels of authorization for payment requests, management approval for outgoing wires, and verification of any changes to vendor data. After the attacks were discovered, the companies reviewed their payment authorization procedures, verification requirements for vendor information changes, account reconciliation procedures and outgoing payment notification processes.

See also "Beware of False Friends: A Hedge Fund Manager's Guide to Social Engineering Fraud" (Mar. 28, 2018).

A New Theory of Cybersecurity Enforcement?

The SEC has traditionally based its cybersecurity enforcement efforts on whether a cyber breach was a "material event" triggering disclosure obligations. However, the SEC has also used a controls-based theory to ground its guidance and enforcement. For registered entities, Regulation SP and Regulation SCI focus on whether the entities have procedures reasonably designed to ensure the security and confidentiality

of customer information. For publicly traded companies generally, the SEC has expressed enforcement interest in controls around systems that contain financial reporting data, insofar that control failures could have a material impact on financial statements. A broader controls-related theory, however, suggests that controls around additional systems could potentially be subject to SEC jurisdiction. The October 16 Report seems to indicate that the SEC may use internal accounting controls requirements of the Securities Exchange Act as the basis for cybersecurity enforcement actions.

See "The SEC's Two Primary Theories in Cybersecurity Enforcement Actions" (Apr. 8, 2015).

Although for public companies that have been victims of BEC scams, the SEC's Report might feel like adding insult to injury, Gesser wrote on Davis Polk's Cyber Blog, it "effectively serves as notice that in the future, a company experiencing a cyber event could later find itself in the SEC's crosshairs."

"The SEC has frequently used the internal accounting controls provisions under 13(b)(2)(B) for FCPA (anti-bribery) enforcement actions, but I'm not aware of those provisions being used for any cybersecurity actions," Gesser told The Cybersecurity Law Report. He further noted that one advantage of the SEC's use of accounting rules "is that they apply to all public companies." In comparison, he pointed out, the SEC's recent action against Voya Financial Advisors, Inc. for weak cybersecurity policies and practices was brought under the Safeguards Rule and the Identity Theft Red Flags Rule, which apply to many investment advisers and broker-dealers that are not publicly traded. The SEC's case against Yahoo! was based on the more traditional disclosure theory, under Section 17(a) of the Securities Act and Section 13(a) of the Securities Exchange Act. "This all shows that the SEC has a lot of tools at its disposal to bring cyber enforcement actions against different kinds of companies in different situations, and it is increasingly willing to do so," Gesser said.

See "SEC Officials Flesh Out Cybersecurity Enforcement and Examination Priorities (Part One of Two)" (May 3, 2017); Part Two (May 17, 2017). See also "SEC $35-Million Yahoo Settlement Carries Breach Disclosure Lessons" (May. 2, 2018).

How to Avoid BEC Scams

Regardless of whether the SEC intends to use this new theory as a basis for enforcement, there is no doubt that BEC scams can expose companies to significant loss. In general, "companies need to make sure that they are keeping up with their expanding cybersecurity regulatory obligations," Gesser advised, "both in terms of any technical requirements, as well as requirements relating to policies, training and testing." To protect themselves against potential losses from BEC scams, he added, companies should consider implementing the following:

- two-factor authentication (including a telephone call from a verified number or an in-person communication) for certain wire instructions and for any changes to wire instructions, including changes to direct deposit instructions for employees;
- training and testing employees involved in payments;
- registering and blocking internet domains that are similar to the company's actual domain name;
- establishing law enforcement contacts; and
- acquiring insurance coverage for losses related to cyber fraud.

Gesser also suggested that companies regularly check for updates from the FBI's Internet Crime Complaint Center on the latest business email compromise scams. The FBI's suggestions for safeguarding against BEC include:

- creating intrusion detection system rules that flag emails with extensions that are similar to company email (for example, if the legitimate company email is abc_company.com, the system would flag an email from abc-company.com);
- creating email rules to flag emails where the "reply" address is different from the "from" address shown; and
- color-coding emails from employee/internal accounts one color and emails from non-employee/external accounts another.