Client Alert

November 2018

SEC Issues Report on Cybersecurity Internal Controls

On October 16, 2018, the Securities and Exchange Commission (SEC) issued a report of investigation entitled "Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements" (the Report). As the latest addition to a growing body of guidance concerning cybersecurity for public companies, the Report reminds businesses that the internal accounting controls required under the federal securities laws should take into account the threat of spoofed or manipulated electronic communications. The Report focuses on a particular kind of cyber scam known as a "business email compromise."

Background

The SEC issued the Report pursuant to Section 21(a) of the Securities Exchange Act of 1934, as amended (Exchange Act). In addition to authorizing the SEC to investigate violations of the federal securities laws, Section 21(a) also permits the agency to issue so-called "reports of investigation," which the SEC does from time to time to educate the market about an emerging enforcement trend when it determines that sanctioning a particular defendant for wrongdoing is not necessary. Indeed, the companies discussed in the Report were not sanctioned.

Here, several public companies each lost millions of dollars as a result of cyber-related frauds. In each case, company employees received spoofed or otherwise compromised electronic communications purporting to be from a company executive or vendor, tricking the employees into initiating wire transfers or paying invoices to accounts controlled by fraudsters rather than legitimate counterparties. According to the SEC, the Federal Bureau of Investigation has estimated that these kinds of business email compromises have caused over $5 billion in losses since 2013, with an additional $675 million in adjusted losses in 2017. In our experience, business email compromises are among the most common types of cyber frauds suffered by businesses of all types.

In connection with the investigations, the SEC considered whether the impacted companies complied with the requirements of Sections 13(b)(2)(B)(i) and (iii) of the Exchange Act, which generally require public companies to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed with, or that access to company assets is permitted only with, management's general or specific authorization. In undertaking this analysis, the SEC emphasized that, while cyber-related threats posed to companies' assets are relatively new, the SEC expects companies to (i) maintain internal accounting controls directed to those risks and (ii) continuously review and update those controls to keep pace with new developments and technologies.

SEC Investigation

The SEC's investigation focused on the internal accounting controls of nine companies that were victims of one of two variants of a business email compromise scheme.[1] Each of the nine companies lost at least $1 million, and two lost more than $30 million. In the aggregate, the nine companies lost nearly $100

[1] According to the SEC, the affected companies covered a range of sectors including technology, machinery, real estate, energy, financial and consumer goods.

million to fraudsters, most of which was never recovered. Some of the investigated companies were victims of ongoing schemes that were uncovered only as a result of third-party actions, such as through detection by a bank or law enforcement agency. For example, one company made 14 wire payments requested by a fake executive over the course of several weeks before the fraud was uncovered by a foreign bank. Another company paid eight invoices over several months in response to a vendor's manipulated electronic documentation for a banking change. The fraud was discovered only when the real vendor complained about past due invoices.

The first type of business email compromise the SEC reviewed involved emails from persons not affiliated with the company purporting to be company executives. In those situations, the perpetrators of the scheme emailed company finance personnel using spoofed email domains and addresses of an executive (typically the CEO) so that it appeared, at least to the casual observer, as if the email were legitimate. In all the frauds, the spoofed email directed the companies' finance personnel to work with a bogus outside attorney who then directed the companies' finance personnel to send large wire transfers to foreign bank accounts controlled by the fraudsters.

According to the SEC, the spoofed emails typically described time-sensitive transactions that needed to be completed within days, and emphasized the need for secrecy from other company employees. They usually requested that wire transfers be made to foreign banks and beneficiaries. The SEC pointed out that, although all the companies had some foreign operations, these kinds of foreign transactions would have been unusual for most of them. The spoofed emails typically were sent to midlevel personnel who generally were not responsible for or involved in the purported transactions, and who usually did not communicate with the executives being spoofed. As is frequently the case in spoofing frauds, the fraudulent emails often included spelling and grammatical errors.

The second type of business email compromise the SEC reviewed involved electronic communications from fraudsters impersonating company vendors. The SEC noted that this variation of the scam is more technologically sophisticated than the spoofed executive emails because, in the instances the SEC reviewed, the schemes involved intrusions into the email accounts of companies' foreign vendors. After hacking the existing vendors' email accounts, the perpetrators inserted illegitimate requests for payments and payment processing details into electronic communications for otherwise legitimate transaction requests. The fraudsters often corresponded with unwitting company employees responsible for procuring goods from the vendors so that they could gain access to information about actual purchase orders and invoices. Typically, the company employee responsible for procurement relayed that information to accounting personnel responsible for maintaining vendor information. As a result, the companies made payments on outstanding invoices to foreign accounts controlled by an impersonator rather than the accounts of the real vendors.

Internal Controls

Section 13(b)(2)(B)(i) and (iii) of the Exchange Act require public companies to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances 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."

The SEC noted that the cases it investigated underscore the importance of devising and maintaining a system of internal accounting controls attuned to cyber-related fraud, as well as the critical role training plays in implementing those controls. The companies here, for instance, had procedures that required certain levels of authorization for payment requests, management approval for outgoing wires and verification of any changes to vendor data, but they still fell victim to these attacks.

In each case, the SEC pointed out that existing controls were interpreted by the companies' employees to mean that the ultimately fraudulent electronic communications were sufficient to process significant wire transfers or changes to vendor banking data. Additionally, many of these companies learned of the fraud

only as a result of third-party notices, such as from law enforcement or foreign banks. The SEC observed that, after falling victim to these frauds, each of the companies enhanced their payment authorization procedures and verification requirements for vendor information changes and improved their account reconciliation procedures and outgoing payment notification processes to aid detection of payments resulting from fraud.

According to the SEC, these business email compromises were successful because the responsible employees 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, the SEC observed that in one case the 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 example, the employee misinterpreted the company's internal authorization policies as giving him approval authority at a level reserved for the CFO.

The SEC also found numerous examples in which the recipients of the fraudulent communications asked no questions about the nature of the supposed transactions, even where such transactions were clearly outside the recipient employee's typical responsibilities and even where the employee was asked to make multiple payments over a period of time. In two instances the SEC found that targeted recipients were themselves executive-level employees—in both cases chief accounting officers—who initiated payments in response to fake executive emails. The SEC observed that, although most of the companies had some form of training regarding controls and information technology in place prior to the scams, all of them enhanced their training of responsible personnel regarding relevant threats and pertinent policies and procedures following the frauds.

Takeaways

Cyber scams like the ones described in the Report are among the many cybersecurity threats faced by today's businesses, including companies subject to the internal controls provisions in the Exchange Act. Many of the frauds the SEC investigated were not sophisticated in design or the use of technology. Instead, as is often the case in cyber attacks, they relied on technology to search for both weaknesses in policies and procedures and human vulnerabilities that rendered the control environment ineffective. According to the SEC, having internal accounting control systems that account for such cyber-related threats and related human vulnerabilities is vital to maintaining a sufficient accounting control environment and safeguarding assets.

The SEC also made clear that having internal controls documented on paper is not enough. Employees must be trained appropriately to implement those controls. As stated above, the Report suggests that, in some instances, a company's documented controls may have been adequate, but the responsible employees did not follow company procedure.

In issuing the Report, the SEC emphasized that it did not mean to suggest that every company that is the victim of a cyber-related scam is automatically in violation of the internal accounting controls requirements of the federal securities laws. Nevertheless, companies' internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds. We expect that internal controls over cyber risks will be the subject of increased scrutiny by the SEC and its staff in the future.

According to the SEC, public companies 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. In particular, the SEC urged companies to evaluate cyber-related threats when devising and maintaining their internal accounting control systems to provide reasonable assurances in safeguarding their assets from these risks.

With the issuance of the Report, the SEC continues its vigilant focus on cybersecurity threats affecting public companies. Given the highly malicious nature of today's cybersecurity environment, we expect the SEC to continue to play a leading role in regulating the cyber practices of US businesses.

Contacts

Brittany M. Bacon
bbacon@HuntonAK.com

Matthew P. Bosher
mbosher@HuntonAK.com

Scott H. Kimpel
skimpel@HuntonAK.com

Lisa J. Sotto
lsotto@HuntonAK.com

Paul M. Tiao
ptiao@HuntonAK.com