LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
WEDNESDAY, JUNE 5, 2019

Cybersecurity and the future of SEC enforcement

By Michael M. Farhang

What responsibilities do U.S. public companies have to prevent theft of company funds through cybercrime? Recent Securities and Exchange Commission guidance suggests that the SEC may be considering a new type of enforcement action to address this question. In October 2018, the SEC issued an investigation report examining nine companies defrauded by cyber-related intrusion and fraud schemes. The report suggests that the agency may adapt an old enforcement tool — the internal controls provision of the federal securities laws — to hold public companies liable when they fail to plan for such schemes. The SEC's new approach would require such companies to undertake proactive steps to build a comprehensive internal controls framework to protect company assets — and by extension, investors — against cyber-related crimes.

The SEC's investigation report examined a common type of cyber-related attack known as the "business email compromise," in which scammers use spoofed or manipulated electronic communications to deceive company employees into misdirecting large amounts of company funds. Business email compromise schemes are often time-intensive, requiring malware or spear-phishing attacks to gain access to a company's network over a period of weeks or months in order to study the company's billing and payment systems, its vendors, and even its executives' email habits. The fraud ultimately occurs with the transmission of fictitious email communications that appear to come from legitimate sources — like company executives or vendors — and contain false instructions that direct unwitting employees to wire or otherwise transfer money to accounts controlled by the scammers.

The SEC found that, in a number of the cases it examined, poor internal risk management policies and procedures, inadequate employee training and awareness, and lax payment authorization and verification processes contributed to the success of the theft schemes. Although the SEC declined to bring enforcement actions against any of the companies, it noted that a public company has an obligation under the federal securities laws, and specifically the internal controls statute, to establish policies and procedures to safeguard company funds against the risk of cyber-related fraud.

The internal controls statute, which was originally passed as part of the U.S. Foreign Corrupt Practices Act of 1977 and is codified at Section 13(b)(2)(B) of the Securities Exchange Act of 1934, has been used repeatedly by the SEC (and in parallel criminal enforcement by the U.S. Department of Justice) to penalize U.S. issuer companies allegedly engaged in foreign bribery. Section 13(b)(2)(B) requires issuers to devise and maintain a system of internal accounting controls sufficient to provide "reasonable assurances" that transactions and access to company assets can occur only with authorization by company management. In a multitude of cases, the SEC has charged companies with internal controls violations as a way to penalize their perceived failure to properly address the risk of bribery by their employees or representatives.

The focus of regulators like the SEC tends to rest on whether a set of controls adequately evaluates and responds to risk, and cyber-related fraud accomplished through spear-phishing, spoofing or email compromises is no different from other areas, e.g., corruption, money laundering, insider trading, etc., in that human error, lack of training, and intentional misconduct lay the groundwork for heightened risk.

Enforcement of Section 13(b)(2)(B) in FCPA cases over the last two decades has led to an evolving set of compliance best practices now familiar to companies and their external counsel that are designed to address the risk that company funds might be used for illicit activity. The SEC has shown a willingness to use Section 13(b)(2)(B) in other contexts as well. The internal controls statute has been invoked to penalize failures to guard against a wide variety of misconduct including fraud, money laundering, and tax avoidance. SEC internal controls enforcement actions have even covered activities as far afield from traditional accounting issues as credit rating practices for mortgage-backed securities and changes to airline routes.

But in the area of cyber-related fraud, how should companies understand their obligations under the SEC's new "internal controls" enforcement approach? The issue is more than just a legal one in light of the financial cost of such fraud. According to the Federal Bureau of Investigation's Internet Crime Complaint Center, business email compromise schemes have caused more than $3 billion in losses to companies, with the numbers skyrocketing — increasing by more than 1,300 percent — since 2015. The SEC has yet to issue clear guidance regarding its views on what constitutes adequate internal controls in this area, but its investigative report suggested that more coherent policies, dedicated and trained personnel, and better screening of payments might have made a difference in some of the cases it examined.

Companies looking to implement robust cybersecurity compliance programs can look to how the SEC has traditionally enforced the internal controls provision in similar contexts, like that of the FCPA. Corruption schemes and cyber-related thefts both involve risks that company funds may be diverted or improperly used, and features typical to FCPA compliance programs— including proper governance and oversight, risk-based policies and procedures, training, vendor and third party controls, self-evaluation, and investigation and remediation processes—can be adapted as areas of emphasis for cybersecurity programs as well.

The focus of regulators like the SEC tends to rest on whether a set of controls adequately evaluates and responds to risk, and cyber-related fraud accomplished through spear-phishing, spoofing or email compromises is no different from other areas, e.g., corruption, money laundering, insider trading, etc., in that human error, lack of training, and intentional misconduct lay the groundwork for heightened risk. Financial Industry Regulatory Authority guidance, for example, reinforces that companies should implement sound governance and risk assessment processes for cybersecurity programs, as well as technical controls and training. The SEC's Office of Compliance Inspections and Examinations issued a 2017 Risk Alert for broker-dealers and investment advisers noting that robust cybersecurity policies and procedures should include risk-based classification of data, monitoring and reporting procedures and controls, mandatory training, and senior management that is engaged and involved in cybersecurity compliance.

The key to understanding how future SEC enforcement will look in this new and evolving area is in the agency's past approaches. The types of cybersecurity programs likely to pass muster in this new enforcement regime are those that take heed of the compliance priorities the SEC has validated in other areas of corporate enforcement while properly adapting them to the new risks posed by cybercrime. Hallmarks like management engagement, proper oversight, clear policies and procedures adapted to risk, training, resources and personnel, ongoing self-assessments, and evaluations of third party compliance are proper starting places. Companies should also bolster their efforts by considering external advisors with expertise in identifying and addressing risk to oversight of company funds. Recent developments show that cybersecurity compliance programs are becoming important not only for avoiding devastating financial losses, but also for avoiding follow-up enforcement action when such losses occur.

Michael M. Farhang *is a former federal prosecutor and partner at Gibson, Dunn & Crutcher LLP. Mr. Farhang has expertise in white collar, securities, and commercial litigation matters and regularly advises corporate and investment clients regarding compliance issues*


FARHANG