PUBLICATIONS

SEC Report on Internal Controls, Cyber-security

November 7, 2018

Thomas O. Gorman

Cyber-security has become – or perhaps should be – a key area of concern for every enterprise. The risks are substantial for the firm, its shareholders, executives and customers as recent cases illustrate. Every enterprise large or small is a potential victim. The losses can and often are substantial not just in dollars but also in trust, customers and more. The Commission has issued guidance. The agency has also brought enforcement actions.

Now, however, the Commission has issued a report based on nine investigations of firms involved in a variety of industries, cautioning about cyber risks in the context of the firm's obligations to maintain proper internal controls. Report of Investigation Pursuant to Section 21(a) of the Exchange Act Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies, October 16, 2018.

Report

The Report involved investigations of issuers in lines of business that ranged from technology, machinery, real estate and energy to financial and consumer goods. Each intrusion centered on the use of email. Each intrusion succeeded in part because of a human component – a lack of training, failure to understand controls or properly apply them. Collectively the companies lost millions of dollars.

The schemes were not sophisticated. The intruders generally employed one of two methods. The first centered on the use of emails from non-affiliates of the firm to company executives using spoofed email domains and addresses. Typically the email went to finance personnel who were directed to coordinate with outside counsel to complete a deal or transaction. The law firm and attorney names were real. Eventually the intruder would claim that there was a time-sensitive deal or that funds were required for a foreign transaction

and request a transfer of funds. The emails in these cases often contained simple errors.

The second centered on impersonating an issuer's vendors. This scheme usually began with identifying venders of the firm, penetrating their system and then forwarding emails to the company. The intruders would typically correspond with issuer personal responsible for procuring goods from vendors. They would be requested to initiate changes to the vendor's banking information. The requests included fraudulent account information. As in the first variation, eventually funds would be wired. Overall the nine issuers involved here lost millions of dollars, most of which have not been recovered.

None of the issuers involved in the underlying investigations were charged. Rather, the investigations are being used to emphasize the fact that cyber-security "presents ongoing risks and threats to our capital markets and to companies operating in all industries. . ." Cyber security risks and management are thus crucial to every issuer. This is particularly true in view of their obligations under Exchange Act section 13(b)(2)(B).

The internal controls provisions of the Exchange Act require that the firm implement a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed in accord with management's authorization and that access to assets is only permitted as authorized. Accordingly, when assessing the adequacy of internal controls, it is imperative to consider cyber-security risks. Those risks are well illustrated by the nine investigations here where the "frauds were not sophisticated. . . [and relied] on technology to search for both weaknesses in policies and procedures and human vulnerabilities that rendered the control environment ineffective." Having systems which factor in cyber-related threats and the related human vulnerabilities, is thus critical, the Report notes.

The Report concludes by noting that "the Commission is not suggesting that every issuer that is the victim of a cyber-related scam is . . . in violation of . . ." the securities laws. Rather, the lesson to be drawn from the Report and the underlying investigations is that "internal accounting controls may need to be reassessed in light of the emerging risks, including risks arising from cyber-related frauds."

Comment

The report repeatedly cites to the history of the internal control provisions and earlier Commission guidance. Viewed in this context the report ties directly to the traditional view of the agency on internal controls. Indeed, that view is frequently seen in financial fraud cases and actions based on the Foreign Corrupt Practices Act.

The report does, however, reach beyond the traditional view of the Commission in this area. A key point of emphasis is the "human" element of controls. This is illustrated in the examples of conduct where there was an intrusion discussed in the Report. The schemes were not sophisticated. There were red flags. Yet the intrusion succeeded because those in charge were fooled, missed the red flags or were not well trained – the human element of internal controls.

While the Report does not develop the "human" element of internal controls in any real sense, the references are noteworthy if for no other reason than this point has traditionally not been emphasized. This human element is in many senses an implementation and training point – properly implementing internal controls requires training and the proper environment. As the examples in the Report illustrate, intrusions are often based on simple schemes. To thwart them, however, there must be proper controls, implemented in an appropriate environment through adequate training – the new element to SEC internal controls.