No. 2018-29
31 October 2018

To the Point

SEC highlights the need for companies to focus on controls that prevent cyber-related fraud

An entity's controls should be designed to address the risk that emails and other electronic communications may not be authentic.

What you need to know

- The SEC issued a report on frauds involving email communications that highlights the need for companies to focus on their procedures and internal controls over the authorization of transfers of cash.
- Many of the frauds described by the SEC were enabled by human actions (or lack of actions) and weaknesses in procedures and controls at companies in a range of industries.
- While the SEC focused on the internal control requirements in federal securities law, management at all entities should be aware of the risks of fraudulent email communications and should consider whether their controls related to the authorization of the transfer of funds and changes to vendor master files would prevent fraud. Management may also want to revisit employee training.

Overview

The Securities and Exchange Commission (SEC) issued a report[1] that highlights the risks companies face related to cyber-related frauds and the need for all companies to consider whether their procedures and controls would prevent losses.

The SEC said it issued the report to make companies aware that cyber-related threats of spoofed or manipulated electronic communications exist and should be considered when a company devises and maintains a system of internal accounting controls, as required by the federal securities laws.

In the report, the SEC noted that companies subject to the internal control requirements[2] are required "... to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed with management's general or specific authorization" and that "... access to company assets is permitted only with management's general or specific authorization."[1]

The SEC said it had investigated whether nine companies that lost a total of nearly $100 million in cyber-related frauds violated the securities laws by failing to have a sufficient system of internal accounting controls, but decided not to pursue enforcement actions against them. The report cited a recent estimate from the Federal Bureau of Investigation that so-called "business email compromises" had caused more than $5 billion in losses since 2013.

Key considerations

The frauds the SEC investigated involved two types of fraud:

- Emails from fake executives — Company personnel received emails that appeared to come from a company executive, typically the chief financial officer. The perpetrators sent emails from a spoofed email domain and address of the executive that instructed the recipient to work with an outside attorney to transfer large sums of money related to time-sensitive transactions or deals that needed to be completed quickly and secretly. The emails typically directed the recipients to transfer funds to foreign banks or beneficiaries.
- Emails from fake vendors — Company personnel received emails that appeared to come from foreign vendors. In these cases, the perpetrators had gained access to the email account of a foreign vendor and used that account to make requests for payments and to request changes to payment information such as bank account numbers. Issuers affected by these schemes typically learned of the erroneous payments when the real vendors followed up on invoices that were still outstanding.

The SEC noted that the frauds were not sophisticated in design or the use of technology. Instead, the SEC said, they used technology to exploit weaknesses in policies and procedures and human vulnerabilities that rendered the controls related to payments ineffective.

How we see it

The pervasive use of electronic forms of communications and the general expectation that such communications are trustworthy creates risks for entities that need to be considered. Entities may need to revisit their controls related to the authorization of the transfer of funds and changes to vendor master file data and their training for employees.

What companies can do

Entities need to reconsider their policies, procedures and related controls to make sure they take into account the possibility that electronic communications may be spoofed or manipulated. That is, entities need to consider whether emails can be accepted as authorization to enter into transactions without additional verification or authentication. Controls that might have prevented the frauds include:

- Requiring that verification of requests for payment above certain thresholds be supported by paper-based documentation
- Requiring that requests for payments from executives be verified by using another form of communication to contact the executive (i.e., not replying to the email containing the request)

- Requiring that requests for changes to vendor master file data be verified by using another form of communication to contact known representatives of the vendor (e.g., a phone call to a predetermined number rather than a response to an email)
- Limiting the number of employees who can make changes to vendor master files or bank routing information
- Confirming outstanding payables with vendors
- Requesting periodic statements from vendors and reconciling the amounts due to the entity's records
- Confirming that security monitoring tools and programs are configured to include email servers to identify suspicious activity such as emails or other communications from unfamiliar internet addresses or messages originating from countries where cybercriminals are known to operate
- Implementing more stringent, incremental controls for payments above predetermined thresholds

Entities may want to consider raising employee awareness of cybercriminals' techniques by conducting more frequent and robust fraud and phishing awareness campaigns and providing comprehensive cyber training.

Further, entities seeking to elevate confidence in their cyber risk management programs have an opportunity to seek an independent, third-party attestation report using the American Institute of Certified Public Accountants' cybersecurity risk management reporting framework.

Endnotes:

1 *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*.

2 Issuers that must comply with Sections 13(b)(2)(B)(i) and (iii) of the Securities Exchange Act of 1934 (the Exchange Act) are those that have a class of securities registered with the SEC under Section 12 of the Exchange Act or that must file reports with the SEC under Section 15(d) of the Exchange Act.