CARTER/LEDYARD

our resources

Cybersecurity: The Weakest Link is Still the People

October 29, 2018

Client Advisory
October 29, 2018 by John M. Griem, Jr., H. Thomas Davis, Jr. and Brielle E. Kilmartin

For ten years the ancient city of Troy was able to withstand a siege by Hellenic armies because of its stout walls and clever, well-armed defenders. What brought down Troy in one night was a single error of judgment.

Three thousand years later, tricking a defender is still the most efficient way to breach strong defenses, including cybersecurity defenses.

Last week the SEC released a cautionary report which described nine successful cyber intrusions against public companies. In each case, a well-meaning employee acting in good faith complied with a request from a "spoofing" email which appeared to be from a company officer or supplier but which was in fact from a thief hoping to breach the company's defenses and rob it.

The Commission investigated whether the targeted companies had complied with the provisions of the Securities Exchange Act of 1934 (Sections 13(b)(2)(B)(i) and (iii), 15 U.S.C. § 78m(b)(2)(B)(i) & (iii)) which require certain issuers to maintain a system of internal accounting controls sufficient to provide reasonable assurances that access to company assets and executed transactions are permitted only with general or specific authorization from company management. While none of these cases resulted in enforcement actions, future companies subject to the Exchange Act that are victims of cyber theft incidents may be required to demonstrate to the SEC that they had internal controls and employee education initiatives to minimize the risk of human error that is the key to these scams.

The targets of these cyber scams included companies from a range of sectors, including technology, real estate, machinery, energy, financial and consumer goods. Two general types of schemes were investigated. The first involved a trickster impersonating an executive within the targeted employee's organization. The second involved a trickster impersonating a vendor seeking a legitimate payment. In each case, an employee either failed to follow company protocol or failed to recognize an apparent red flag. All of the investigated companies suffered monetary loss as a result of these impersonation schemes.

I. Scheme #1: The CEO Needs My Help and Fast!

The first type of scam involved the impersonation of an executive within the organization. A person not affiliated with the company but purporting to be a company executive emails company finance personnel using spoofed email domains and addresses of an executive, typically the CEO. The targeted employee is typically a mid-level finance employee who does not usually communicate with the spoofed executive directly. The employee is instructed to initiate wire transfers to foreign bank accounts controlled by the tricksters. These schemes often claim there are time-sensitive transactions with foreign beneficiaries, a claimed "need for secrecy", claims of government oversight and a lack of transaction details. The spoofed emails were not sophisticated in design or use of elaborate technology. In fact, they required nothing more than creating an email address to mimic the executive's address.

II. Scheme #2: The Outstanding Vendor Invoice; Pay it Now…..and Also Pay it Later….

In a second scheme, the trickster infiltrated vendor e-mail accounts, giving these emails a more sophisticated appearance. After hacking the vendor accounts, the fraudster sent illegitimate payment requests in the form of purchase orders or invoices to the company. The procurement employees who received the invoice provided the payment request to the finance department and paid the "outstanding invoice" directly to the perpetrator's foreign bank account. The SEC noted that because of the long cycle between payments, it often took longer to discover the problem in these cases.

Both types of schemes involved several red flags and employee mistakes. In most cases, human error made the attempted cyber heist a success. Common employee mistakes included:

- Failure to follow dual-authorization wire payment requirements;
- Misinterpretation of the company's payment authorization payment matrix;
- Failure to ask questions about a transaction that was not within the employee's typical area of responsibility.

Red flags in the spoofing emails included:

- Spelling and grammatical errors, including in the email address the message was delivered from;
- Directions to send funds to offshore accounts;
- Claimed need for secrecy;
- Claimed time sensitivity for an unspecified transaction;
- Assertion that the funds were needed for a foreign transaction with minimal details regarding the transaction.

Every type of business is a potential target for these attacks. Every business should evaluate both its internal accounting controls and employee understanding and implementation of controls and similar measures. Specifically, companies should assess whether new policies and/or policy enhancements are necessary in the areas of:

- Payment authorization;
- Verification for vendor information changes;
- Account reconciliation processes;
- Payment notification processes.

Most importantly, companies should increase employee cyber-fraud training across all levels of the company. Training should include education on the types of prevalent cyber threats which employees may encounter, as well as typical red flags to watch out for and periodic refresher courses in company policies and procedures. Spoofing is a common threat and can be easily avoided.

III. Conclusion

Cyber threats and criminal behavior are constantly evolving. The SEC's report serves as yet another reminder to companies of the importance of proactively evaluating and improving internal controls coupled with employee training to better understand how to handle the problem if

and when it arises. Proactively improving internal controls, and reviewing agreements with key vendors and others who have access to a company's information technology systems, will also reduce the risk of litigation and business disruption arising from cyber scams.

The best advice a company can give its well-meaning employees is to pay attention, watch for red flags, and trust your intuition. If something seems "fishy", it probably is!

Questions regarding this advisory should be addressed to **Jack Griem** (212-238-8659, griem@clm.com), **Tom Davis** (212-238-8850, davis@clm.com), **Brielle Kilmartin** (212-238-8652, kilmartin@clm.com), or your regular Carter Ledyard attorney.

---

related professionals

John M. Griem, Jr. / Partner
D 212-238-8659
griem@clm.com

H. Thomas Davis, Jr. / Partner
D 212-238-8850
davis@clm.com