Adding Insult to Injury: SEC Warns That Cyber Incidents May Lead to Enforcement Action

October 18, 2018

On Tuesday the Securities and Exchange Commission issued a **Section 21(a) report of investigation** emphasizing the importance of assessing the likelihood of cyberattacks when designing internal accounting controls and conducting training for personnel responsible for their implementation. The SEC's enforcement division examined incidents at nine unnamed public companies that had been victims of cyber fraud, resulting in aggregate losses of approximately $100 million. Each incident involved a "business email compromise" or "phishing" scheme in which employees were tricked into wiring money to accounts controlled by bad actors posing as company executives or vendors. The SEC investigated the companies' compliance with provisions of the Securities Exchange Act of 1934 requiring maintenance of a system of internal accounting controls that give reasonable assurance that company assets are only accessible in accordance with management's authorization. While the SEC concluded that enforcement action was not warranted against the companies, which spanned industries including financial services, consumer goods and machinery, the regulator warned that internal accounting controls "may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds." The report thus effectively serves as notice that in the future, a company experiencing a cyber event could later find itself in the SEC's crosshairs.

Two types of schemes were investigated:

- **Email from a fake executive**

  In this type of fraud, the perpetrators emailed personnel of a company's finance department using a spoofed email domain purporting to be the address of a company executive, often the CEO. The emails sometimes directed finance department employees to work with outside attorneys and send wire transfers to foreign bank accounts controlled by the perpetrators. The outside attorneys appeared to work for real law firms, but telephone calls to them were answered by skilled impersonators. The communications were usually urgent in nature and concerned time-sensitive "deals," some of which even purported to be under SEC oversight. Most transfers were made to foreign banks, and while the companies did have foreign operations, the transactions were nevertheless out of the ordinary and thus might have raised red flags. Additional warning signs included the fact that the emails were sent to mid-level employees who rarely interacted with the purported senior-level senders, and featured numerous grammatical and spelling errors. The SEC noted that these spoof emails were not sophisticated from a technological point of view.

- **Email from a third-party vendor**

  In the second type of fraud, emails purporting to originate from a company's vendor instead were the product of hacking into the vendor's email account and falsifying payment details in what otherwise appeared to be legitimate payment requests. These emails were more technologically sophisticated and had fewer warning signs than the fake executive emails, and were revealed to have been fraudulent when the actual vendors sought payment.

The SEC has previously counseled public companies on their disclosure obligations relating to cybersecurity risks, as we discussed in our February 2018 **memo**. Yesterday's report focuses not on a company's public disclosures, but on its internal operations – its books and records. The regulator cautioned that public companies should pay close attention to their obligation to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that . . . transactions

are executed in accordance with management's general or specific authorization" and that "access to assets is permitted only in accordance with management's general or specific authorization." The SEC emphasized the importance of taking into account both cybersecurity threats and "related human vulnerabilities" when designing these controls, since cyberattacks need not be particularly sophisticated to cause significant harm through clever exploitation of human weaknesses. In a recent **SEC settlement order**, the SEC found that Voya Financial Advisors Inc. did not have reasonable cybersecurity policies and procedures in place to detect identity theft risks or respond to cybersecurity attacks, resulting in a $1 million penalty and an agreement to retain an independent consultant to review its policies and procedures for compliance with the Safeguards Rule and the Identity Theft Red Flags Rule, even though there was no finding of harm to any customers. The SEC likely expects companies to review their controls and procedures, including employee training, to see what may need to be strengthened in order to defend against the ever-evolving cyber threat matrix.

* * *

Some measures that companies can consider implementing to reduce the risk of falling victim to a business email compromise scheme include:

- **Two-factor authentication for certain wire instructions**

  Consider establishing an alternate communication channel, other than email (such as telephone calls or in-person communications), to verify significant wire transactions, as well as any changes to wire account instructions, including changes to direct deposit instructions for employees. When using phone verification as part of the authentication procedure, consider only using previously known phone numbers, not numbers provided in an e-mail request.

- **Phishing training and testing**

  Consider training and testing for employees involved in payments to raise awareness about common phishing schemes and educate them on cybercrime prevention.

- **Look-alike company domains**

  Consider registering and blocking Internet domains that are similar to the company's actual domain name (e.g., davisp0lk.com, davispo1k.com, davispollk.com).

- **Establish law enforcement contacts**

  Consider establishing a law enforcement cyber contact, which can help companies effectively respond to fraudulent transfers more quickly once they are discovered.

- **Insurance coverage**

  Determine whether your insurance would provide coverage for a business email compromise, and if not, whether to obtain coverage.

- **Check for updates on the latest business email compromise scams**

  Consider having someone at the company monitor **www.ic3.gov** for updates on new variations of these scams and other internet crimes, and educate company leaders and employees on the latest recommended best practices.

- **Notification of auditors and audit committee**

  Consider notifying the auditors and audit committee of any such cyber events since internal controls are often implicated.

Similar tips and resources to assist our clients in their efforts to maintain compliance with their cybersecurity regulatory obligations are now available through the **Davis Polk Cyber Portal**.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Richard D. Truesdell, Jr.	**212-450-4674**	**richard.truesdell@davispolk.com**
Michael Kaplan	**212-450-4111**	**michael.kaplan@davispolk.com**
Joseph A. Hall	**212-450-4565**	**joseph.hall@davispolk.com**
Bruce K. Dallas	**650-752-2022**	**bruce.dallas@davispolk.com**
Sarah K. Solum	**650-752-2011**	**sarah.solum@davispolk.com**
Avi Gesser	**212-450-4181**	**avi.gesser@davispolk.com**
Li He	**011-852-2533-3306**	**li.he@davispolk.com**