October 18, 2018

Cybersecurity Update: SEC Releases Report of Investigation into Internal Controls at Public Company Victims of Cybercrime

Public companies are increasingly targeted by cyber criminals even as they navigate the tension between regulators recognizing them as victims versus viewing them as bad actors. This week, the Securities and Exchange Commission issued an investigative report assessing whether nine public companies victimized by cyber-related fraud had failed to implement and maintain adequate internal controls that, in theory, could have protected them. In the wake of the SEC's recent cybersecurity disclosure guidance and enforcement actions earlier this year after data breaches at public companies and an investment adviser, the report confirms that cybersecurity remains an SEC enforcement priority.

The investigation focused on issuers that had fallen victim to a widespread and relatively unsophisticated form of cybercrime known as "business email compromise," in which cyber criminals impersonate either company executives or company vendors and send emails to finance personnel requesting large wire transfers to foreign bank accounts. After failing to detect the spoofed or compromised nature of the email requests, the nine victim companies transferred a total of nearly $100 million to cyber criminals.

Though the SEC ultimately determined not to pursue any enforcement action, its report serves as notice to all public companies that the Commission may consider such charges in the future. Public companies should take heed of the "cyber-related threats of spoofed or manipulated electronic communications"—which the FBI reports have caused over $5 billion in losses since 2013—and consider those threats carefully "when devising and maintaining a system of internal accounting controls as required by the federal securities laws."

Notably, while the SEC's investigation may have revealed some control weaknesses, the criminals also succeeded because they convinced company personnel to circumvent existing controls or act beyond their authority. In addition to updating internal controls regularly in light of the shifting risk environment, companies should proactively train personnel to reduce human errors that criminals may exploit to bypass controls and safeguards designed to thwart cybercrime.

Wayne M. Carlin
Sabastian V. Niles
Marshall L. Miller
Courtney L. Shike