Cyber Breaches and Insider Trading

By Charles Elson and Sanjai Bhagat, Ph.D.

Listen to article

100

There's a better way to prevent C-Suite self-dealing than the SEC's cybersecurity disclosure proposal.

The SEC is currently considering rules concerning cybersecurity incident disclosure. The proposed rules would require current reporting about material cybersecurity incidents and periodic updates about previously reported incidents and the company's procedures to identify and manage cybersecurity risks.

The SEC's concern for timely disclosure to investors would prevent insiders (the company's senior executives) from trading on this information before the public disclosure of the cybersecurity incident. This concern is not just hypothetical. During the summer of 2017, Equifax was the victim of a data breach, during which hackers acquired the key data of over 145 million Americans. Before the breach was made public, Equifax's CIO sold almost all of his shareholdings in the company. Subsequently, the CIO was criminally prosecuted for insider trading and sentenced to jail. The Equifax episode is not an isolated incident. A recent paper in the *Journal of Financial Markets* documents several hundred instances in the past decade during which insiders sold significant amounts of stock after they became aware of a serious cybersecurity lapse in their respective companies, but before announcing these cybersecurity lapses to the general public. Relatedly, a recent *Review of Accounting Studies* paper documents that CEOs whose compensation is more heavily weighted with equity-intensive compensation are more likely to delay the disclosure of major cybersecurity lapses.

The SEC’s concern regarding timely disclosure of cybersecurity incidents is legitimate. However, this problem is better addressed by changing the incentive compensation plan for senior executives.

We propose that the incentive compensation of senior corporate executives should consist primarily of restricted equity (i.e., restricted stock and restricted stock options). The executive cannot sell the shares or exercise the options for six to 12 months after their last day in office. This would eliminate the ability of executives to engage in insider trading related to the cybersecurity incident.

In an earlier article, we discuss the pros and cons of the restricted equity incentive compensation plans. Briefly, if executives are required to hold restricted shares and options, their savings would most likely be under-diversified and they would be concerned with lack of liquidity. To address these concerns, we recommend the amounts of equity awarded under our proposal should be increased slightly from current levels in order to bring the risk-adjusted expected return back up. Additionally, managers should be allowed to liquidate annually, on board approval, a modest and minimal fraction of their awarded incentive restricted shares and options.

We applaud the motivation for the SEC’s concern regarding increased disclosure requirements associated with cybersecurity incidents. However, instead of additional regulations, these concerns can be more effectively addressed by corporate boards that adopt the above restricted equity incentive compensation plan. Furthermore, our proposal would also address the concern that making cybersecurity incident disclosures within four days could interfere with the company’s attempts at cybersecurity defense to address the incident as well as law enforcement’s investigation and enforcement.

Charles Elson is executive editor-at-large of Directors & Boards*. He is a director of Blue Bell Creameries Inc. and Enhabit Home Health and Hospice Inc.*

Sanjai Bhagat, Ph.D., is a director of ProLink Solutions and provost professor of finance at the University of Colorado at Boulder.