CYBERSECURITY: GROWING CONCERN FOR THE GOING CONCERN

Cybersecurity is not a new topic, but its importance has grown exponentially with the number of sophisticated data security breaches reported in the last five years. These breaches have become a multi-million dollar problem for many organizations such as Target, Chase, Ashley Madison and Equifax. With more exposure on the topic coming from the seemingly unending investigation into Russia's meddling with the 2016 election, we now know more than we ever have about cyber attacks and the risks they pose. Even with that knowledge, however, it seems as though there is no way to prevent these attacks from happening.

The Securities and Exchange Commission (SEC) may have had that thought in mind last month when it released a Statement and Guidance on Public Company Cybersecurity Disclosures. This Statement is undoubtedly SEC's way of saying, if we can't stop the attacks, we must be prepared to handle them correctly.

2011 Guidelines

On October 13, 2011, the SEC released a statement to provide guidance on disclosure obligations relating to cybersecurity risks and cyber incidents. In their statement, the SEC stated that companies need to "*disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky.*" There was nothing in their statement providing guidance on how detailed these disclosures needed to be. As a result, according to a 2014 study by PricewaterhouseCoopers and the Investor Responsibility Research Center Institute, the disclosures that companies made based on these guidelines were not useful.[1]

The main criticism stemmed from the lack of depth provided in the SEC guidelines. What would happen if a company failed to comply with the SEC's expectations as set forth in their statement? The recent Equifax breach that affected almost 150 million people occurred in July, but the company did not make the disclosure until September. They did not meet the SEC's expectations of making a timely disclosure, yet they were not penalized for doing so.

The timing of the SEC's guidelines last month gives us reason to believe that it was in response to Equifax's poor disclosure procedure following their breach. However, after reading the new guidelines, they seem to miss the mark yet again.

New Guidelines

Since the release of the new guidelines on February 20, 2018, companies have not been in any rush to change their current disclosure procedures. Based upon what has been learned over the last seven years in relation to cybersecurity, it is disappointing to see how little the guidelines differed from those given in 2011.

The guidelines offer a basis to build a company's or bank's disclosure, such as the importance of having in place "*disclosure controls and procedures that provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition and results of operations.*" They also provide for an expectation to "*disclose cybersecurity risks and incidents that are material to*

[1] https://irrcinstitute.org/wp-content/uploads/2015/09/cybersecurity-july-20141.pdf.

investors, including the concomitant financial, legal or reputational consequences." However, the verdict is still out on what the repercussions will be for ignoring these guidelines.

The SEC is calling for more detail in the companies' disclosures of cybersecurity risks by making reference to the financial, legal and reputational factors, yet no new consequences for failing to do so. Even some within the SEC, like Commissioners Kara Stein and Robert Jackson, are disappointed with the statement. Commissioner Stein believes that these new guidelines provided *"modest changes"* at best, while Commissioner Jackson stated that it *"essentially reiterates years-old staff-level views on this issue."*[2] If the SEC's own commissioners are not standing behind the new guidelines, what makes them think that companies and banks will start investing more time, effort and resources into cybersecurity.

Insider Trading

One of the main takeaways from the new guidelines was the provision on insider trading. The SEC does not present new laws or regulations on the topic, only provides that companies and their executives *"should be mindful of complying with the laws related to insider trading in connection with information about cybersecurity risks and incidents, including vulnerabilities and breaches."*

This again provides evidence that the guidelines were a direct response to the Equifax breach. During the six weeks between the breach and the disclosure, the Chief Financial Officer and three other executives sold securities worth $1.8 million.[3] Though there has been no evidence that the individuals knew about the breach at the time of trading, one can begin to speculate. Even though the SEC makes reference to such laws, again it is without any additional merit. Companies and their executives have always been aware of the laws of insider trading, the SEC guidelines stating that they *"should be mindful"* of those laws provides for nothing more than a reminder.

How to React

Cybersecurity is not going anywhere. It is a threat that will continue to intimidate every company and bank that has confidential information stored online. Though the takeaways from the new guidelines are minimal, cybersecurity should without a doubt be a top concern for each and every organization. Companies and banks need not change policies just because a statement was issued, but should continuously amend their policies based on the ever-changing risks in the market and state regulations. In Florida, Section 501.171, Florida Statutes, governs how corporations and banks should handle disclosures.

For questions or concerns regarding compliance, contact us here.

Nicholas A. Colella
Attorney with Igler | Pearlman, P.A.
2075 Centre Pointe Blvd., Suite 100
Tallahassee, FL 32308
(850) 878-2411
Nick.Colella@IglerLaw.com

[2] https://www.csoonline.com/article/3260006/data-breach/secs-new-cybersecurity-guidance-falls-short.html.

[3] https://www.ctvnews.ca/business/equifax-calls-executive-stock-sales-days-after-breach-legal-1.3662082.