SEC Concerns On Cybersecurity

by Matthew Rossi, Laura D. Richman and Melanie M. Burke

Cybersecurity and its related liabilities have forced digital oversight onto every board's agenda. However, the direct losses from digital mischief are only one area of danger. The SEC has shown growing concern about digital security over the past decade, and a new guidance policy earlier this year compels boards of public companies to ask tough new questions. Are our cyber disclosure policies adequate? Further, can we assure that no inside traders will try to profit from an incident?

The cybersecurity landscape is evolving more rapidly than ever, and the threats to businesses' critical information and assets are increasing. Cybersecurity threats come from a wide range of sources, including foreign and domestic hackers, traders and others who traffic in stolen market-moving information, prospective market manipulators, and state-sponsored actors.

Some of the world's largest corporations have been hurt by cybersecurity breaches, and these continue to grow in scale and sophistication. Thus, in the wake of a cyber incident, the question for many public corporations becomes "what do we need to tell the investing public?" The Securities and Exchange Commission has now provided its most detailed guidance to date to assist public companies wrestling with this question.

In February 2018, the SEC issued guidance to aid public companies in addressing cybersecurity risks and incidents. The 2018 SEC guidance makes clear that disclosures regarding cybersecurity are of paramount importance to the SEC, stating "the commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion..." As cyber threats continue to plague corporations at home and abroad, the SEC is keeping close watch on how corporations respond to these incidents.

Over the last several years, the SEC has increasingly focused on cyber threats and their corresponding impact on corporations, investors, and the general public. In 2011, the SEC's Division of Corporation Finance staff issued disclosure guidance regarding cybersecurity. This 2011 staff guidance explained that existing disclosure requirements may impose an obligation on issuers to disclose significant cybersecurity risks and incidents.

In June 2017, Stephanie Avakian and Steven Peikin were named the new co-directors of the SEC Division of Enforcement. Following their appointment, Peikin and Avakian made clear that cybersecurity would remain a high enforcement priority at the SEC. Peikin was quoted as saying that "the greatest threat to our markets right now is the cyber threat." Similarly, Avakian noted that there has been a recent "uptick" in cybercrime investigations and added that she anticipates seeing "the cyber threat continue to emerge" in coming years.

SEC Chairman Clayton wants "more and better" cyber disclosure, warning that the SEC "will investigate issuers that mislead investors about material cybersecurity risks or data breaches."

In September 2017, the SEC announced the creation of a Cyber Unit within the Division of Enforcement aimed at combating cyber-related misconduct, including market manipulation, hacking, dark web misconduct, and violations related to initial coin offerings. Significantly, this newly created Cyber Unit also investigates cases involving cyber-related disclosure failures by public companies. Earlier this year, the SEC imposed a $35 million penalty on the company formerly known as Yahoo! for failing to timely disclose a data breach. According to the

Matthew Rossi *is a partner,* **Laura D. Richman** *is counsel, and* **Melanie M. Burke** *is a former associate of the Mayer Brown law firm. [www.mayerbrown.com]*

SEC, although information relating to the breach was reported internally to members of the company's senior managment and legal department, the company failed to properly investigate the circumstances of the breach and to adequately consider whether the breach needed to be disclosed to investors.

Chairman Clayton has made clear that "[t]he Commission is focused on identifying and managing cybersecurity risks and ensuring that market participants—including issuers, intermediaries, investors and government authorities—are actively and effectively engaged in this effort and are appropriately informing investors and other market participants of these risks." He has repeatedly called for public companies to make "more and better" disclosure in this area, warning that the SEC "will investigate issuers that mislead investors about material cybersecurity risks or data breaches."

The new guidance emphasizes the importance of timely disclosure, and suggested more information about the range and financial impact of cybersecurity incidents.

The 2018 SEC guidance reemphasized the SEC's vigorous commitment to cybersecurity disclosures and policies. The statement explicitly addressed two topics not addressed in the 2011 guidance on the topic. First, the importance of implementing cybersecurity policies and procedures; and second, the application of insider trading prohibitions in the cybersecurity context.

SEC Chairman Jay Clayton noted that he expects the 2018 SEC guidance "will promote clearer and more robust disclosure by companies about cybersecurity risks," and that as companies implement it, the SEC will consider "whether any further guidance or rules are needed."

The 2018 SEC guidance reiterates that companies should consider the materiality of cybersecurity risks and incidents when preparing disclosures for registration statements. The 2018 guidance goes on to specify that "[t]he materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the scope of business operations." Materiality "also depends on the range of harm that such incidents could cause."

The new guidance also emphasizes the importance of timely disclosures, and suggested that corporations should incorporate into their financial statements information about the range and financial impact of cybersecurity incidents on a timely basis "as the information becomes available." The SEC expressly stated that a corporation's establishment of an internal investigation into cyber risks and incidents does not by itself obviate the need to disclose information to the public. This is a key takeaway for corporations attempting to address cyber threats.

The 2018 SEC guidance emphasizes that there are a number of areas in which disclosure of cybersecurity risks and incidents may be required, depending on the particular facts and circumstances. These include business and operations, risk factors, legal proceedings, management's discussion and analysis, financial statements, disclosure controls and procedures, and corporate governance.

The 2018 SEC guidance suggests that companies should consider the following issues when evaluating cybersecurity disclosures:

- Prior cybersecurity incidents, including their severity and frequency.
- The probability of the occurrence and potential magnitude of cybersecurity incidents.
- The adequacy of preventative actions, and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks.
- Company business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third party supplier and service provider risks.
- The costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers.
- The potential for reputational harm.
- Existing or pending laws and regulations that

may affect companies relating to cybersecurity and the associated costs.

□ Litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

The 2018 SEC guidance also mentions that the disclosure of the board's role in risk oversight, which is part of the proxy statement disclosure requirements, should include a discussion of the board's role in overseeing the management of cybersecurity risks if such risks are material to a company's business.

Cyber disclosure should "allow investors to assess how a board of directors is discharging its risk oversight responsibility."

The SEC believes that "disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area."

In its statement, the SEC made clear that effective and wide-ranging cybersecurity policies and procedures are of utmost importance. SEC Chairman Clayton "urge[d] public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives."

SEC Commissioner Kara Stein also noted in her own statement that "[t]oo many companies currently fail to consider cybersecurity as a business risk and, thus, do not incorporate it within the risk management framework overseen by their boards." In light of the SEC guidance, boards should prioritize the implementation of cyber policies and procedures.

Companies should assess whether their current disclosure controls and procedures are adequate to assure timely disclosure of cybersecurity risks and incidents emphasized in the SEC guidance. Also, periodically evaluate whether those controls and procedures remain adequate.

Companies should also consider whether they need to revise their insider trading policies and procedures to specifically address prohibitions on insider trading as they apply to cybersecurity. The 2018 SEC guidance strongly advises public companies to maintain policies and procedures that address this risk of illicit trading.

Boards should evaluate whether they are sufficiently involved in the oversight of cybersecurity risks and whether they need additional training in this area. Companies preparing proxy statements should consider discussing board oversight of cybersecurity risk as part of their discussion of the board's role in risk oversight.

Companies should consider how they will address any public disclosure obligations in response to a cybersecurity incident. The SEC guidance recognizes that "it may be necessary to cooperate with law enforcement," but nonetheless states that an ongoing internal or external investigation into an incident does not itself justify a delay in public disclosure.

This approach puts the guidance in some tension with many state data breach laws. These allow a company to refrain from notifying consumers of an incident at the request of law enforcement, or while an investigation of the scope of a breach is ongoing.

Following a cybersecurity incident, be vigilant to avoid insiders trading in company securities while in possession of material nonpublic information.

Companies should weigh how to manage these differing disclosure obligations in a manner that minimizes legal risk and reputational harm (by preventing undue delay between a public disclosure to investors and subsequent breach notifications). Moreover, companies must bear in mind that a new incident may require them to revisit disclosures previously made to investors.

Following a cybersecurity incident, companies should also be vigilant to avoid corporate insiders trading in company securities while in possession of material nonpublic information. Companies in this situation may want to prohibit trading by corporate insiders under such circumstances.

Similarly, persons should not enter into or alter Rule 10b5-1 trading plans while in possession of such information. In addition, corporate insiders with pre-existing Rule 10b5-1 trading plans should consider the optics of having trades occur pursuant to a trading plan before disclosure of a cyber incident. While trading pursuant to such plans may not violate insider trading laws, it may generate negative publicity for both the insider and the corporation.

The SEC has now made clear that corporations that do not comply with its cybersecurity recommendations may be subject to enforcement actions.

Perhaps the most significant development to come out of the 2018 SEC guidance is the cautionary notice regarding insider trading liability with knowledge of an undisclosed cybersecurity incident. The classic theory of insider trading prohibits corporate insiders, such as directors and officers, from trading in a corporation's securities on the basis of "material, non-public information" about the corporation.

The SEC advised that "companies would be well served by considering how to avoid the appearance of improper trading during the period following an incident."

The 2018 SEC guidance expressly applied this traditional framework to non-public information about cybersecurity threats or incidents. It explicitly states that "information about a company's cybersecurity risks and incidents may be material nonpublic information, and directors, officers, and other corporate insiders would violate the antifraud provisions if they trade the company's securities in breach of their duty of trust or confidence while in possession of that material nonpublic information."

This would mean, for example, that if a director or officer was aware of a major data breach and sold company stock because of that knowledge, he or she could be prosecuted for insider trading. The new SEC guidance encourages companies to consider how their codes of ethics and insider trading policies take into account and prevent trading on this basis.

The SEC advised that it believes that "companies would be well served by considering how to avoid the appearance of improper trading during the period following an incident and prior to the dissemination of disclosure."

More than this, the SEC advised that "[p]ublic companies should have policies and procedures in place to: (1) guard against directors, officers, and other corporate insiders taking advantage of the period between the company's discovery of a cybersecu-

What Can Your Company Do?
Suggested Policies And Procedures

With cybersecurity policies and procedures at the forefront of the 2018 SEC guidance, what policies and procedures a company can implement to comply with the increased demands on corporations? Some suggested policies:

- ☐ Develop a response strategy for ransomware incidents.
- ☐ Develop and follow information governance controls, including upward reporting.
- ☐ Identify, map, and assess compliance with legal and regulatory obligations and determine cyber vulnerabilities and risks.
- ☐ Establish a work plan for cybersecurity crisis prevention and management.
- ☐ Implement strategies for industry information sharing and government and law enforcement coordination.
- ☐ Develop and maintain written policies and procedures.
- ☐ Also develop and maintain training programs for employees and contractors.
- ☐ Deploy appropriate information security safeguards for vendors/service providers, including reporting and due diligence.
- ☐ Regularly confirm implementation of secure technology and corresponding updates.
- ☐ Identify and pre-position forensic, legal and PR consulting and other outside resources.
- ☐ Regularly test and update all assessments, safeguards, and protocols.
- ☐ Conduct regular tabletop exercises.
- ☐ Detect and remediate advanced persistent threats.
- ☐ Monitor and communicate periodic alerts on new and existing threats throughout the organization.

rity incident and public disclosure of the incident to trade on material nonpublic information about the incident, and (2) help ensure that the company makes timely disclosure of any related material nonpublic information."

This demonstrates the SEC's concern related to cybersecurity. The guidance specifies that the SEC expects companies "to have policies and procedures to ensure that any disclosures of material nonpublic information related to cybersecurity risks and incidents are not made selectively, and that any Regulation FD required public disclosure is made simultaneously (in the case of an intentional disclosure as defined in the rule) or promptly (in the case of a non-intentional disclosure) and is otherwise compliant with the requirements of that regulation."

Adoption of the 2018 guidance by the full SEC may signal that potential legal liability of corporations and individual directors for cybersecurity-related issues may have increased. It is imperative that in response, corporations and their boards actively communicate with counsel to limit legal exposure and avoid cybersecurity pitfalls.

While the full impact and practical effects of the 2018 SEC guidance remain to be seen, it is clear that corporations must now address more carefully than ever before cybersecurity risks, policies, and reporting. The SEC has made clear corporations can no longer ignore these issues without repercussion. The onus is on corporations and their counsel to prioritize cybersecurity and stay abreast of further developments in this area. ■

Reprinted by THE CORPORATE BOARD
4440 Hagadorn Road
Okemos, MI 48864-2414, (517) 336-1700
www.corporateboard.com