SEC Requires Greater Transparency On Companies' Efforts To Prevent Cyberattacks

By **DON CARPENTER**, MSAcc/CPA

It is now a regular occurrence to read of yet another company that has experienced a breach in its defenses against cyberattacks. Data such as confidential customer information is repeatedly compromised. The disclosure earlier this year that client information in Facebook had been "mined" and used by Cambridge Analytica in the most recent presidential election campaign made front page news. The incident dominated headlines as Facebook Chairman and CEO Mark Zuckerberg testified before Congress regarding steps his organization would take to remediate its systems and prevent similar breaches in the future.

Breaches in information technology systems can occur due to intentional malicious third-party efforts, negligence on the part of employees, or system glitches or failures. But regardless of the cause, the fallout of lapses in data security can be very costly and result in harmful consequences, including the following:

- Lost revenue due to customer defections and damage to market reputation,
- Costly settlements with those adversely affected and regulatory agencies,
- Remediation costs, such as systems upgrades and added personnel to prevent future attacks.

Don Carpenter is clinical professor of accounting at Baylor University. Contact him at Don_Carpenter@baylor.edu.

Given the ever-increasing automation and interdependence of business systems, the Securities and Exchange Commission (SEC) released interpretive guidance earlier this year that requires companies to include cybersecurity in their disclosure policies and procedures. It is important to distinguish the policies and procedures that companies adopt to detect and prevent system breaches from those that are the focus of the SEC release. The SEC is requiring companies to review and update disclosure policies and procedures that relate to their reporting obligations as public companies.

A review of the required risk factors in annual reports will indicate that most companies have determined that cybersecurity is material enough to warrant inclusion. However, the SEC is now saying that the reporting obligation extends beyond just describing the risks of cyberattacks. The guidance requires review of the following four areas of corporate governance.

1. Policies and Procedures

A registrant's disclosure obligations in its annual and quarterly reports require information from all parts of the organization. The financial statements form the backbone of the reports, but these are fleshed out in the footnotes and MD&A. To ensure that all relevant information is assimilated on a timely basis, detailed protocols are followed as the books are closed. For example, it is often standard practice for the reporting team to hold discussions with counsel to ascertain if disputes or litigation should be disclosed even if accruals are not required. Similar procedures are followed for other areas requiring potential disclosures.

Likewise, building a protocol to capture all relevant information regarding cyber occurrences and modifications the company has made to its technology security is now required. Documenting the company's decision regarding when and to the extent disclosure is necessary, as well as the concurrence of the company's audit firm on a timely basis, is also advisable.

2. Extent of Disclosure Obligations

The SEC also stressed that the disclosure obligation of registrants extends beyond the Risk Factor section of the annual report. Companies should consider the costs of cybersecurity measures, the frequency and costs of breaches and other incidents, and the potential for future incidents in the preparation of MD&A. To the extent that the costs and risks fall disproportionately among the reportable segments, this should also be disclosed.

The financial statement footnotes should align with the increased transparency of MD&A. The impact of cybersecurity incidents on revenue and the value of intangible customer relationships should be discussed, if material. In addition, settlement costs for disputes stemming from breach of contracts or indemnifications and insurance costs should be disclosed if material.

3. Board Oversight

The guidance also reminds registrants that the extent of its board of directors' participation in the oversight of risk is required to be disclosed. This disclosure is often included in the company's annual proxy statement. As cybersecurity has continued to increase in materiality, companies may find it necessary to include a review of their cyber policies and procedures, as well as incidents, on the agendas of directors' meetings on a regularly recurring basis.

4. Reporting and Insider Trading

The SEC also included a reminder that directors, officers and other insiders must be mindful of rules relating to insider trading. It is illegal to trade in securities if one is in possession of material nonpublic information. Details about cybersecurity incidents could qualify as such information. And the disclosure of such information also falls within the purview of Regulation FD, which requires that any selective disclosure of nonpublic information must be made available to the investing public. In this context, it is also advisable to consider the use of Form 8-K that requires the disclosure of major or material events within four days of occurrence, with regard to cybersecurity issues.

The focus of the SEC on cybersecurity in the context of its reporting and disclosure framework confirms the increased importance and corresponding risks inherent in this vital part of organizations.