Yahoo Inc. was fined a US$35 million penalty for failing to disclose one of the largest data breaches in the world, in which hackers captured the personal data of millions of user accounts. The failure to disclose the breach misled investors. The breach originally occurred in December 2014, when Yahoo's information security group discovered that Russian hackers stole what was identified internally as the crown jewels of the company. The breach was reported internally to both senior management and Yahoo's legal department, who failed to investigate and disclose the breach to the public in 2014. It was disclosed two years later, in 2016. In fact, there was not any timely disclosure reported on any previously filed interim Form 8-K (current), Form 10-Q (quarterly) or Form 10-K (annual) report, resulting in the US Securities and Exchange Commission (SEC) enforcement action.1

In response to the increasing threat of cybersecurity breaches, the SEC issued CF Disclosure Guidance: Topic No. 2—Cybersecurity on 11 October 2011. It provides a framework for public organizations in the United States and their foreign subsidiaries to disclose their cybersecurity-related information.2 Although the guidance is not the official SEC ruling, failure to comply may have adverse consequences, as evidenced by subsequent SEC enforcement and examination actions.

The 2011 guidance provides a clear road map for organizations to assess and disclose their cybersecurity risk systematically. These disclosures give information to the market that can help investors become aware of the enterprise's cybersecurity environment, possible cyberattacks identified and the potential risk associated with their securities investments. This guidance started the route for public organizations regarding their disclosure obligations focusing on cybersecurity risk and incidents. For example, the Marriott Starwood breach, disclosed in November 2018, resulted in the value of its shares declining by 6 percent. As a result, this important information disclosed to stockholders by the SEC assisted in the investors' investment decisions. As organizations rely more on the Internet to operate, the risk of cybersecurity breaches continues to rise.3

In response to these breaches and nondisclosure issues, the SEC voted unanimously on 20 February 2018 to upgrade the 2011 guidance to help public enterprises prepare cybersecurity disclosures involving risk and incidents. As a reinforcement and expansion to the 2011 guidance, the SEC adopted “Commission Statement and Guidance on Public Company Cybersecurity Disclosures” on 26 February 2018.4 This new statement's goal is to promote clearer and more vigorous disclosures about cybersecurity, the risk factors and incidents.5 It requires organizations to provide additional detailed information on cybersecurity to ensure a balance between the capital markets and the protection of investors. The statement issued by the SEC not only aims to strengthen the regulator's stand on public organizations' obligations under current US security laws to disclose cybersecurity risk and incidents, but it also helps to inform investors about risk and breaches in a timely manner to assist in their short-and long-term decision-making.
The 2018 statement expands mandated cybersecurity disclosures through the authority of the SEC. The 2011-issued guidance from staff emphasized that organizations may be obligated to disclose cybersecurity risk and incidents, while the 2018 statement provides specific disclosure requirements. The statement emphasizes the importance of cybersecurity policies and procedures. The SEC now requires enterprises to disclose cybersecurity risk and material incidents including legal, financial or reputational consequences. The SEC considers information to be material if a reasonable investor considers the information important in making an investment decision. Also, the 2018 statement focuses on enterprises examining their internal accounting controls. In addition, the 2018 statement emphasizes the prohibition of insider trading prior to disclosure to the public.

Although the 2018 statement is meant for US public enterprises, the compliance impact goes beyond borders. Besides the statement applying to US corporations, it also applies to their foreign subsidiaries. Furthermore, cybercrimes these days go beyond any physical borders, and organizations can be affected by cyberincidents no matter their physical location. Even for organizations that do not participate in American equity markets, the SEC’s cybersecurity reporting requirement is a summary of best practices in dealing with cyberincidents, so IT and security professionals should be aware of the compliance trend and consider the SEC requirements as their internal roadmap to combat cybercrimes.

It is important to note that both the 2011 guidance and the 2018 statement recognize that managers, directors, officers and other persons responsible for developing and overseeing such controls and procedures have discretion in developing their disclosure strategy. The SEC acknowledges that disclosing too much or being too specific about cybersecurity incidents may have an adverse effect, where the disclosures provide a road map for hackers to use in launching attacks. It is important to find the balance between being a good corporate citizen by not withholding critical information while protecting shareholder interest. Developing a good strategy to manage cybersecurity risk is a top priority for IT professionals and board members in today’s connected business world.

Both the 2011 guidance and the 2018 statement highlight the structure organizations can use to fulfill their disclosure obligations related to cybersecurity, but how are they different? What prompted the SEC to elevate its cybersecurity disclosure requirements, and how should organizations implement these enhanced disclosures? An explanation of the differences between the 2011 guidance and the 2018 statement assists organizations in understanding their SEC compliance with regard to risk disclosures and cybersecurity. It also provides guidance to board members, IT professionals and accounting personnel.

“IT IS IMPORTANT TO FIND THE BALANCE BETWEEN BEING A GOOD CORPORATE CITIZEN BY NOT WITHHOLDING CRITICAL INFORMATION WHILE PROTECTING SHAREHOLDER INTEREST.”

Publication Hierarchy
The first notable change involved the transformation of a staff opinion in 2011 to the disclosure requirement becoming an official SEC statement in 2018. The 2011 guidance represents viewpoints from the staff of the Corporate Finance Division, one of the five divisions of the SEC. The 2018 statement represents the official stand of the commission, which represents the regulator’s emphasis on the need for public enterprises to disclose cybersecurity issues to comply with Regulation Fair Disclosure.

Cyberattack Landscape
As cybercriminals become more sophisticated, the risk that enterprises face and the cost implied to manage or mitigate these risk factors has skyrocketed in the last few years. The 2018 statement recognizes the complicated nature of today’s cyber threat landscape. In addition to deliberate attacks or unintentional events that lead to the disruption of enterprise operations or theft of organization assets or data, the 2018 statement
concedes that the cyberattacks can be carried out by organized penetrators such as nation-states or hacktivists, using means including phishing, malware or ransomware to gain unauthorized access. The costs associated with cyberattacks are much more complicated as well.

**Disclosure Controls**

The most significant new development in the 2018 statement is the emphasis on enterprises’ policies and procedures (or lack thereof) to deal with cybersecurity and disclosure controls. The original 2011 guidance directs organizations to disclose material cybersecurity risk and incidents. The new statement goes a step further to state that not only are enterprises required to disclose material cybersecurity risk and incidents, but they also need to do it in a timely fashion.

The SEC encourages organizations to promptly disclose a cybersecurity incident within four days by using a current report such as the Form 8-K and also requires duplicated filing in the periodic report Form 10-Q (quarterly) and Form 10-K (annual), previously mandated by the guidance. Form 8-K is the timely current report to file when a breach has occurred. This report is labeled a current report because it can be filed anytime to meet the timely deadline to disclose material events, corporate changes or important information that the organization is required to make public prior to the filing of the next Form 10-Q (quarterly) or Form 10-K (annual) report. As management consults with legal counsel on when and what to disclose when a breach is detected, organizations need to have policies and procedures to make sure this delicate balance between timely disclosure obligations and legal challenges is maintained.

The 2018 statement identifies the framework that addresses the following:

- Involving the board in its administration of risk oversight function, i.e., how does the board exercise its oversight of the organization’s management team when cybersecurity risk is material to the enterprise’s operations
- Allowing chief executive and financial officers to exercise their obligations to certify cybersecurity risk and incident disclosures

In addition to the not specific but material information disclosure requirement, the 2018 statement put a significant emphasis on timeliness. The SEC requires the organization to file known material events within four business days. The Form 8-K is the current report that best satisfies this requirement on a timely basis, unless the Form 10-Q (quarterly) is published in the next four days to the stockholders. The information must also be stated in the Form 10-K (annual) at the end of the year.

It is worth noting that just like the 2011 guidance, the 2018 statement does not mandate that enterprises provide detailed technical disclosures that could compromise their cybersecurity efforts. What is essential in disclosing cybersecurity risk and incidents is to apply the framework mentioned previously to determine whether the information to be disclosed is material and to ensure that organizations do not overlook any material information in these disclosures. The SEC recognizes that organizations may not have a complete picture when a breach is just discovered, and internal or external investigations may be ongoing; therefore, organizations are allowed to update or refresh previously made disclosures, but they are still obligated to provide timely disclosures.

**Disclosure Vehicles**

The 2011 guidance mainly suggests that enterprises use period reports such as the Form 10-
K (annual) and Form 10-Q (quarterly) to disclose cybersecurity risk and incidents in the discussions of risk factors, management discussion and analysis, description of business, legal proceedings, and financial statement disclosures. However, since timely disclosure is the new emphasis in the 2018 statement, the newly added disclosure vehicles include reporting in a current report (Form 8-K), news release, and to report on the discussions of internal controls to address disclosure controls and procedures designed specifically for cybersecurity risk and incidents. An example of a recent current Form 8-K filed by Capital One as a result of a major breach detected on 19 July 2019 can be found at the SEC’s EDGAR company filing database. This archived file of Form 8-K for Capital One details the data security incident, including the occurrence of the event, the filing date of the Form 8-K, the vulnerability that led to the incident, the discovery of the incident, how the event happened and the financial impact. Note that the event occurred on 22 March 2019, but awareness did not happen until the filing date of the report of 19 July 2019.

Insider Trading
The statement also defines the rule on insider trading. The insider trading rule primarily indicates that steps must be taken to prevent directors, officers and other insiders of the enterprise from trading the organization’s stock until investors are appropriately notified. The rule emphasizes that it is illegal to trade a security based on material nonpublic information involving cybersecurity risk and incidents. Information about an organization’s cybersecurity risk and incidents may be material nonpublic information. As a result, directors, officers and corporate insiders would violate the antifraud provisions by trading the organization’s securities in breach of their duty of trust. The statement encourages organizations to review their code of ethics for policies that promote compliance with applicable laws, including those prohibiting insider trading.

Critical Role for Public Organizations
The most important impact for public organizations as a result of the 2018 statement is in the review of their formal governance hierarchy. The board of directors (BoD) must position cybersecurity as a top-priority matter on their agenda. Board members must be educated with the SEC’s new statement in assisting to manage and enrich their overseeing of cybersecurity risk and incidents, in addition to confirming that policies and procedures exist within the corporate structure. Also recommended is the creation of a cybersecurity committee within the BoD to access enterprise risk relating to cybersecurity.

"SENIOR MANAGEMENT MUST HAVE ADEQUATE INFORMATION IN ANALYZING AND DECIDING ON MATERIAL DISCLOSURE DECISIONS."

Another impact of the 2018 statement is the importance of the involvement of the audit committee in their role involving cybersecurity. In this respect, the audit committee must work with Certified Public Accountants (CPAs) who are auditors of financial statements, internal audit directors, trusted advisors who are experts in governance and risk, and business executives such as chief executive officers (CEOs) and chief financial officers (CFOs) for advice on how to manage cybersecurity responsibilities. Senior management must have adequate information in analyzing and deciding on material disclosure decisions. Continual communication must be open between these parties.

A public organization affected by the statement must provide ongoing training exercises for their employees. As a result of the increased use of digital technologies to conduct daily operations, it is critical that all employees become involved in cybersecurity management. Another important impact is in the development of strong internal controls. These examples accentuate the importance of training employees in the development and maintenance of an internal accounting control system that assists in monitoring cyber-related threats and aids in having an efficient and effective accounting control environment.
It is evident that public enterprises will be impacted by the SEC’s 2018 statement and create a strategy designed to assist in preventing, detecting and responding to cybersecurity threats. This strategy impacts the whole organization structure, ranging from the BoD to all employees in the organization. It is imperative that public organizations develop policies and procedures to ensure timely disclosures of material nonpublic information involving cyberattacks. It is also critical that actions be taken to prevent any insider trading.

The Evolution of the SEC Rules

The move from the 2011 guidance to the 2018 statement represents the reignited emphasis of the regulator’s stand on balancing cybersecurity risk management and the public’s right to know. Knowing the evolution of the SEC’s stand on cybersecurity disclosure requirements helps organizations understand the mandate today.

Figure 1 highlights the differences between the two SEC publications.

It is important to note that the 2011 guidance and the 2018 statement discussed here focus on SEC disclosures involving risk and incidents only for US domestic public organizations and their foreign subsidiaries.

There is no doubt that the SEC must have a key role in the cybersecurity of US public enterprises and their foreign subsidiaries. The 2018 SEC statement has become an important regulation to assist public enterprises in preparing and presenting disclosures about cybersecurity risk, incidents and insider trading. Cybersecurity risk presents serious threats to countries, capital markets and investors. Organizations are challenged in the landscape of cybersecurity threats, where hackers utilize a maze of tactics to commit cyberattacks. These may include phishing, malware, ransomware, stolen

| Figure 1—The Differences Between US SEC’s 2011 Guidance and 2018 Statement |
|-------------------------------------------------------------|-----------------------------------------------------------------------|
| **The 2011 Guidance**                                        | **The 2018 Statement**                                                |
| Publication hierarchy                                        | The 2011 publication represents a staff opinion. It presents the first comprehensive guidance on how public organizations address and report cybersecurity risk and incidents. |
| Description of cyberattack landscape                        | In addition to traditional hackers, the perpetrators can involve nation-states or hacktivists. The attack is not limited to gaining unauthorized access or data theft. With a goal to interrupt operations; it could be aimed at destroying infrastructure. |
| Disclosure controls and procedures                         | The disclosure controls and procedures serve as part of the overall corporate governance mechanism. Organizations should make sure that a clear reporting chain is defined and used in the event of a breach and senior managers have the right amount of information to make materiality determination and disclosure decisions. In addition, how the board is involved in the governance of cybersecurity risk management should be documented. |
| Disclosure vehicles                                         | In addition to period reports, organizations are asked to utilize a current report, such as Form 8-K, to improve the timeliness of cybersecurity incident disclosures. |
| Insider trading                                             | Enterprises should implement policies on insider trading during and after cybersecurity incidents. |
access credentials, distributed denial-of-service attacks and Structured Query Language (SQL) injection attacks. The cost to these public organizations for increased cybersecurity protection expenses involve personnel (including accounting and IT), training, and consultant costs. In addition, other incurred remediation costs, lost revenues, legal fees and regulatory actions can be substantial and provide negative consequences for a public enterprise.

Cybersecurity protection is more critical today as a result of public organizations’ business operations increasing their dependence on digital technologies and electronic communication. This has also increased the risk related to cybersecurity when business transactions and assets become more vulnerable to different cyber-related threats. As a result, there has been an increase in more recurrent and serious cyberincidents.

Throughout the years, the SEC has questioned the accuracy of disclosures in terms of completeness and timing. Public enterprises must review the adequacy of their disclosures relating to cybersecurity risk and incidents similar to reviewing other operational and financial risk. It is highly recommended that public enterprises create a strategy designed to assist in preventing, detecting and responding to cybersecurity threats. It is imperative that public organizations develop policies and procedures to ensure timely disclosures of material nonpublic information involving cyberattacks.

According to the US Securities and Exchange Act of 1934, public enterprises must continually review and adjust their internal accounting controls to the current risk environment. SEC Chairman Jay Clayton said, “Investors rely on our public issuers to put in place, monitor, and update internal accounting controls that appropriately address these threats.” Internal accounting controls play a vital role in the public enterprise’s management of risk approach to cyberthreats and in the protection of investors. Factoring cyber-related threats into the internal control system is important to the control environment and asset safeguarding.

Conclusion

As an initial path to proper management of cybersecurity-related disclosure strategy, it is imperative that board members always have cybersecurity on their agenda and approach it as an enterprise-wide risk. Directors must also have access to cybersecurity expertise with regular and adequate time devoted to cyber risk management at board meetings. Also, board members must confirm that adequate budget and staff exist to help in the cyber risk management framework. Also recommended is the creation of a cybersecurity committee within the BoD to assess enterprise risk relating to cybersecurity. It is also important that audit committees of public organizations become involved in cybersecurity. In this respect, the audit committee must work with IT professionals who are auditors and consultants of governing the organization’s IT assets, and resources and business executives, such as CFOs, for advice on how to manage cybersecurity responsibilities. Continual communication must be open between these parties.

Because of technological advancements and the fact that cybercriminals are getting more sophisticated, it can be expected that the cyberattack landscape and its impact on business and investors will become more complicated. Public organizations have an obligation to disclose material information, and it is essential that when enterprises invest in strategies to cope with cybersecurity, they do not overlook the importance of disclosure controls and include cybersecurity management in the overall corporate governance mechanism.
Endnotes


6 Ibid.

7 Regulation Fair Disclosure, or Regulation FD, is an SEC rule that aims at preventing from selective disclosures. The idea is that when publicly traded organizations disclose a material information to selected parties, that same information must be made available to the general public as well.


9 Op cit US Securities and Exchange Commission, 16 October 2018

10 Grant, G. H.; C. Grant; "SEC Cybersecurity Disclosure Guidance Is Quickly Becoming a Requirement," The CPA Journal, May 2014, p. 69–71