We saw in the lesson some companies like to be very detailed in their 10-K information about security, others prefer brevity.  How specific should companies be in their descriptions of cybersecurity in their 10-K reports? What are the drawbacks and benefits of providing these details?

The Securities and Exchange Act of 1934, which was intended to regulate publicly traded companies provides the Securities and Exchange Commission (SEC) the authority to oversee the comprehensive annual financial report also known as the 10-K. The SEC requires companies to file for this report to increase transparency so that current and investors can make informed decisions based on their knowledge of the company’s business, operations, finances, and risks. However, neither the Act of 1934 nor the SEC’s regulation S-K explicitly requires companies to disclose cybersecurity risks in their 10-k reports. Nevertheless, the SEC imposes several disclosure requirements that require companies to disclose cybersecurity risks and vulnerabilities (Kosseff, 2017).

In practice, companies must disclose cybersecurity risks and vulnerabilities in four sections of their annual 10-k reports which include: risk factors, management’s discussion and analysis of financial condition and results of operations (MD&A), description of their business, and legal proceedings (Kosseff, 2017). However, when it comes to how specific companies should be in their descriptions of cybersecurity in the 10-K reports, it really depends on the company’s business and cybersecurity issues. For example, Walmart’s 2016 10-k filing was extensive in part due to the large amount of sensitive consumer data it handles. On the other hand, Berkshire Hathway’s 2016 10-k filing was short since the company doesn’t deal with consumers (Kosseff, 2017). Hence, as applicable, companies must provide a complete description of the risks, including information about prior cybersecurity incidents where there may have been data loss. They might also include the severity, the frequency, the probability and magnitude of future risks. Additionally, they should present selected financial data that explains either good or bad performance over the previous year. They should also report unusual or infrequent events or transactions or any significant economic changes that materially affected the amount of reported income from continuing operations.

The benefits of providing these details are that it increases investors' awareness of the nature of the risks faced by the organizations. On the other hand, the drawbacks of providing these details are that if companies expose enough information, there is a risk of compromise of their cybersecurity to hackers (Securities and Exchange Commission, 2018). Hence companies should follow a balanced approach when preparing their 10-k reports. That is, they shouldn’t have little detail that it doesn't adequately describe the risks associated with that cybersecurity framework. At the same time, they shouldn’t provide enough detail for somebody outside the company to use that information to launch an attack against them.

References

Kosseff, J. (2017). Cybersecurity Law. Hoboken, N.J: John Wiley & Sons, Inc.

Securities and Exchange Commission. (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Retrieved from https://www.sec.gov/rules/interp/2018/33-10459.pdf