Reflections on SEC Cybersecurity Guidance

The Rise of the Investor in the Cybersecurity Discussion

February 28, 2018
Evolver, Inc.
Over the past year, the cybersecurity world has undergone a major shift as cyber attacks have transitioned from “potential” losses to a company to direct, near term losses for major corporations. From the recalling of hundreds of thousands of medical devices to ransomware attacks that have shut down major facilities, the cyber losses are directly hitting companies’ revenue and value. These losses have now caught the attention of the investment community with a growing cry for visibility into a company’s risk as a result of a cyber attack.

The big shoe dropped last week when the SEC released: Commission Statement and Guidance on Public Company Cybersecurity Disclosures, a new guidance for public company reporting on cyber security risk. The guidance is a major expansion of previous guidance on how cyber risk should be reported and is ushering in a new world of how investors, corporations, law firms, and regulators will address cybersecurity in their everyday operations.

The Cases Driving the Change

Cybersecurity breaches have been around for a long time. Everybody remembers the Target and Home Depot incidents, which exposed thousands of customers’ credit card data. Though these breaches were large in scale, a case could be made that they had little material impact. The attacks targeted the companies’ payment card systems, but did not affect the ability of Target or Home Depot to deliver their products. Some would say that there was a small hit to corporate reputation, but looking at the stock values of the companies since the breaches, one could also say they were not material to long-term operations.

What has changed in the past 18 months is that there have been a number of cases and incidents that have had direct and material impact on the companies under attack. These material events go to the investors’ interest, and is a driving factor in the new direction set out by the SEC in support of the investment community. A summary of some of these major cases is below, and, surprisingly, it does not start with Equifax.

**Yahoo** – In the middle of an acquisition by Verizon, Yahoo announced that they had a major breach compromising over a billion accounts. The resulting action was for Verizon to reportedly drop the price for Yahoo by $350M.

**St. Jude Medical** – In the middle of an acquisition by Abbot Labs, an investment firm, Muddy Waters, reported that St. Jude’s medical devices had severe cybersecurity issues that would have a significant financial impact on the company. At one point, the value of St. Jude dropped by as much as eight percent. Soon after, the FDA joined in on the device complaint. In the end, Abbott had to recall over 450,000 devices.

**Merck** – There is probably no better example of the SEC interest in financial reporting than the Merck situation from the middle of 2017. In 2017, Merck posted this in their 3rd quarter 8-K SEC filing:

*Sales in the third quarter of 2017 were reduced by approximately $240 million due to a borrowing from the U.S. Centers for Disease Control and Prevention Pediatric Vaccine Stockpile of GARDASIL 9 (Human Papillomavirus 9-valent Vaccine, Recombinant), a vaccine to prevent certain cancers and other diseases caused by HPV, driven in part by the temporary production shutdown resulting from the cyberattack, as well as overall higher demand than originally planned.*
Additionally, as expected, revenue was unfavorably impacted by approximately $135 million from lost sales in certain markets related to the cyber-attack.

Though there was general discussion that the NotPetya attack had impacted Merck, the severity of the attack was not really announced until this SEC report. Interestingly, Merck’s fourth quarter report listed the following forward looking statement on risks:

*Risks and uncertainties include but are not limited to, general industry conditions and competition; general economic factors, including interest rate and currency exchange rate fluctuations; the impact of pharmaceutical industry regulation and health care legislation in the United States and internationally; global trends toward health care cost containment; technological advances, new products and patents attained by competitors; challenges inherent in new product development, including obtaining regulatory approval; the company’s ability to accurately predict future market conditions; manufacturing difficulties or delays; financial instability of international economies and sovereign risk; dependence on the effectiveness of the company’s patents and other protections for innovative products; and the exposure to litigation, including patent litigation, and/or regulatory actions.*

Even after last year’s cyber attack, Merck does not specifically list another attack as a possible future risk. The Merck story caught enough attention to result in a letter from Congress (view article).

**Equifax** – No cyber assessment can be written without a mention of Equifax. The potential harm to the continued operations of the company remains in discussion. The fact that a major threat to sensitive consumer data was not listed as a threat to the overall status and revenue of the company in previous disclosure statements has drawn the interest of investors, regulators, and Congress.

**Express Scripts** - This is a case that many may not be aware of because, as far as current information indicates, there has not been a breach. The New York State Comptroller is trying to force a prescription benefits company, Express Scripts Holding Co., to release information on how they are reducing cyber security risks (view article). The action, according to Comptroller Thomas DiNapoli, is in the interest of investors. Additionally, DiNapoli has requested the SEC weigh in and force Express Scripts to disclose the information. Mr. DiNapoli is acting as a shareholder in this situation as the New York State Common Retirement Fund holds about $164M in Express Scripts stock.

**The SEC Weighs In**

Given the backdrop of a number of companies exposed to material impacts due to cyber attacks, the SEC released new guidance on how companies should disclose this risk. Cybersecurity has been a disclosable item since 2011, but as shown in the Merck example above, the detail and method of this reporting has been minimal at best. The new guidance from the SEC significantly expands the recommended detail to be disclosed by public companies in the course of their ongoing operations. As stated in the guidance:
Item 503(c) of Regulation S-K and Item 3.D of Form 20-F require companies to disclose the most significant factors that make investments in the company’s securities speculative or risky. Companies should disclose the risks associated with cybersecurity and cybersecurity incidents if these risks are among such factors, including risks that arise in connection with acquisitions.

It would be helpful for companies to consider the following issues, among others, in evaluating cybersecurity risk factor disclosure:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;
- the probability of the occurrence and potential magnitude of cybersecurity incidents;
- the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company’s ability to prevent or mitigate certain cybersecurity risks;
- the aspects of the company’s 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 the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

There are a lot of other aspects to the guidance that include considerations related to mergers and acquisition, past events, and overall market conditions.

One interesting element of the SEC guidance is the focus on the impacts of cybersecurity on business factors and cost. This is a major departure for most companies that leave the management of cybersecurity to the technical side of the company. This guidance suddenly brings all parts of the company, from accounting through outside counsel, into the discussion. Additionally, as an SEC disclosure statement, the information provided holds the company accountable to how the cyber risk calculations are made.

The Quantification of Cyber Risk

Though the SEC guidance places a much greater emphasis on the reporting of cyber risk, the move is in line with the rapidly changing way cybersecurity is being evaluated in many companies. Over the past 24 months, there has been a major move toward calculating cyber risk in monetary terms. Many major corporations are now using an international standard known as the Factor Analysis of Information Risk (FAIR). The move to FAIR by companies such as Bank of America and Walmart has assisted executives in logical decision making. The SEC guidance will only accelerate the move to measuring cyber risk in monetary terms.
A reflection of the move toward monetary measurement and management of cyber risk is the growth of the FAIR Institute, a non-profit industry group of companies performing quantification of risk through the use of the model. Though only in existence for two years, the industry group now has over 2500 members with expectations of reaching 4000 by the end of the year. Another sign of the move toward FAIR and monetary measurement has been the adoption and instruction by major universities such as Carnegie Mellon.

The challenge that follows the SEC guidance is: exactly what does a viable disclosure report look like that meets the guidance provided by the SEC? By its nature, cybersecurity is a continuously changing landscape. And how does a company reveal possible risks without exposing their cyber weaknesses? Consider the St. Jude case mentioned above. The company’s products were shown to have major vulnerabilities, but what is the responsibility of the company to reveal these weaknesses?

**Rise of the Investors**

The actions of the New York State Comptroller and the SEC will influence the disclosure by companies of their cyber risks. The question remains, how does that influence investors? The disclosure of major cyber weaknesses in a product should definitely give an investor pause. But what about organizations such as financial institutions, healthcare companies, and entertainment firms? The long term threat to these companies for having cyber weaknesses is less obvious. Remember, Merck was not a target of the NotPetya virus, they just got it as it ran through the internet.

As these regulatory bodies pay closer attention to cyber risk, even more questions about the details of such disclosure arise. How do large corporations disclose where the cyber risk lies? And, would such a disclosure influence buying decisions by investors? How do these disclosures influence where companies spend their money, more on cybersecurity and less on functionality?

All of these questions will be addressed in the upcoming months. There is no doubt that the SEC guidance will change the cyber risk conversation in companies from a pure technical to a technical/monetary discussion. Audit committees and law firms will be searching for experts in how to generate the types of disclosures the SEC desires and the SEC will likely be asked for greater discussion and clarification. Also, investor advocate groups and law firms are going to be reviewing these disclosures to see if the reports sufficiently address the risks being placed on the investors. The next six months will be interesting as these items are worked out in boardrooms across the country.

---

**About the Author**

Chip Block is Vice President of Evolver, Inc., (www.evolverinc.com) a major supplier of cybersecurity and infrastructure services to the commercial and public sectors. Mr. Block has worked extensively in the cyber research, development, and operations field for over fifteen years and been awarded several high level honors for his advanced technological achievements. He is a frequent speaker at technology conferences on cybersecurity, cyber risk, and cyber insurance. He is the architect of the Cyber Risk Ecosystem and has authored several whitepapers including “And then the Accountants Showed Up: How the Insurance Industry Will Drive Cybersecurity” and “The Solution to Medical Device Security Also Could Save Tens of Thousands of Lives and Millions of Dollars”.

5 | Reflections on SEC Cybersecurity Guidance