Bloomberg Law®

Privacy and Security Law Report®

VOL. 17, NO. 66 329-368 APRIL 9, 2018

# Public Companies Should Update Cybersecurity Risk Disclosures

The Securities and Exchange Commission was careful to note that it does not expect public companies to make their disclosure so detailed as to provide a ''roadmap'' to cyber criminals to bypass a company's protective measures, write Edward Normandin and Matthew Repetto of Pryor Cashman LLP. As such, the SEC acknowledges that disclosure of specific technical information about cybersecurity systems or system vulnerabilities is not expected, they write.

BY EDWARD NORMANDIN AND MATTHEW REPETTO

With the increasing frequency of significant cybersecurity breaches affecting high-profile public companies (e.g., Equifax, Uber, Yahoo, Target, eBay) and in light of the recent Securities and Exchange Commission guidance on public company cybersecurity risk, public companies would be well-served to give fresh consideration to their cybersecurity risks and the adequacy of their current disclosure (e.g., in annual reports and registration statements).

*Edward Normandin is a partner in Pryor Cashman's nationally recognized Corporate Group, where he represents businesses at all stages of growth, from startup ventures to publicly traded corporations. Normandin often serves as outside general counsel to clients, advising on matters ranging from corporate organization and governance to regulatory compliance.*

*Matthew Repetto is a member of Pryor Cashman's Corporate and Investment Management Groups, where he advises public and private companies on a broad range of transactions and general corporate matters, including acquisitions, mergers, entity formation, and financings.*

In recognition of the changing cybersecurity landscape and attendant risks to public companies, the SEC on Feb. 21, 2018, released new guidance on cybersecurity disclosure requirements for public companies. This new guidance was widely anticipated by securities law practitioners following the SEC chairman's published remarks in September 2017, and it provides a long-overdue update to the SEC's 2011 initial guidance on cybersecurity risk. Although no formal rules were promulgated by the SEC at this time, the new guidance sets out the SEC's current expectations for cybersecurity risk disclosure by public companies which, if not heeded, could potentially result in enforcement actions, SEC comments on securities filings, and/or shareholder lawsuits.

Regulation S-K, which sets forth the rules for disclosures in public company filings, requires public companies, with some exceptions, to disclose in a separately captioned ''Risk Factors'' section ''the most significant factors that make an investment in a registrant's securities speculative or risky.'' This section typically includes

 ISSN 1538-3423

an extensive set of risk factors disclosing a variety of risks that company management deems material. Following the SEC's initial cybersecurity guidance in 2011, in which it encouraged public companies to consider the materiality of risks related to cyberattacks and subsequently make the appropriate disclosures, public companies seemed to respond in one of several ways. Some elected to provide a specific, sometimes standalone cybersecurity risk factor in their public filings, while others continued to rely on broadly worded risk factors designed to cover a variety of general information technology, data or systems-related risks. Still, many companies elected not to supplement their risk factors to address cybersecurity risk. Regardless of a public company's current cybersecurity risk disclosure practices, it is likely that the new SEC guidance has rendered such disclosure inadequate for the purpose of properly informing investors of material cybersecurity risks. We believe that, generally, there is much room for improvement in cybersecurity risk disclosure, and we expect to see improvements made soon, as public companies and their securities counsel digest the new guidance and the SEC begins to use its powers to encourage greater disclosure.

This article highlights aspects of the SEC's latest guidance on cybersecurity risk factor disclosure and outlines considerations public companies should weigh when crafting their own cybersecurity risk factors.

## Highlights of SEC's Guidance

The SEC states that its new guidance is meant to promote clearer and more robust cybersecurity risk disclosure to protect investors from potential consequences of a public company cybersecurity breach. As noted in the new guidance, these consequences include lost revenue, increased costs for protection, remediation costs, reputational damage, organizational changes, increased insurance premiums, legal claims, regulatory actions, and damage to a company's stock price and long-term shareholder value. Because of the seriousness of these consequences, the SEC has taken the stance that it is ''critical that public companies take all required actions to inform investors about significant and material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to cybersecurity risks but have not yet been the target of a cyber-attack.''

To help public companies determine what may be a ''significant cybersecurity risk'' for purposes of evaluating their cybersecurity risk factor disclosure, the SEC listed the following considerations:

- the severity and frequency of incidents;
- probability of occurrence and potential magnitude;
- adequacy of preventative actions;
- aspects of the company's business that may give rise to potential risks;
- potential costs;
- potential reputational harm;
- existing or pending laws; and
- litigation or regulatory investigations.

The SEC also reminded public companies that they are required to disclose ''such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading.'' In determining what may be considered ''material,'' the SEC invokes a standard of materiality consistent with the Supreme Court's standard in *TSC Industries v. Northway*, which states that a cybersecurity risk or incident is material ''if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available.''

When providing these disclosures, the SEC emphasized, as it has many times before, that a ''company-by-company'' approach to disclosure is expected. This is important because every company has a different risk profile, and these differences should be reflected in risk factor disclosures. Accordingly, companies are advised to avoid generic cybersecurity-related disclosures or boilerplate, and instead, provide specific information that is useful to investors. However, the SEC was careful to note that it does not expect public companies to make their disclosure so detailed as to provide a ''roadmap'' to cyber criminals to bypass a company's protective measures. As such, the SEC acknowledges that disclosure of specific technical information about cybersecurity systems or system vulnerabilities is not expected.

It should be noted that the new SEC guidance expands on its 2011 guidance by addressing two new topics: the importance of cybersecurity policies and procedures, and the application of insider trading prohibitions in the cybersecurity context. We encourage public companies to review the SEC's new guidance and become familiar with its additional expectations.

## Key Takeaways

We advise public companies seeking to improve their disclosure of *material* cybersecurity risks and meet the SEC's expectations for clearer and more robust disclosure to consider the following suggestions when crafting their cybersecurity risk factor disclosure.

*1. Add a stand-alone cybersecurity risk factor.*

Strong consideration should be given to providing a stand-alone cybersecurity risk factor in annual reports and registration statements. Although the SEC guidance stopped short of mandating any new disclosure category for cybersecurity risk, the SEC has clearly signaled to public companies that current cybersecurity risk factors need greater clarification of the nature and type of risk and the potential consequences. A standalone risk factor will provide an opportunity for more in-depth discussion of the particular cybersecurity risks faced by the company, the probability of incident, the potential impact of an incident and any past cybersecu-



  PVLR ISSN 1538-3423

rity incidents affecting the company, its customers, vendors or competitors, and any risk prevention measures undertaken. A stand-alone risk factor may also demonstrate the company's recognition of the seriousness of cybersecurity risk and perhaps provide some reassurance to investors, the SEC, and governance watchdogs that the company's management is taking measures to prevent a breach incident and/or will not be completely caught off guard if an incident occurs. In addition, a stand-alone risk factor increases the prominence of the disclosure in the company's filing, thus allowing investors to more easily spot the potential material cybersecurity risks and make more informed investment decisions.

*2. Avoid using boilerplate cybersecurity risk factors.*

Following the SEC's 2011 guidance, some public companies responded by adding carefully crafted and tailored risk disclosure to their filings. However, many others responded simply by adding generic or ''boilerplate'' risk factor disclosure often borrowed from the filings of larger companies which were not tailored to their own business and circumstances, including, in some cases, borrowing from companies in different industries and/or with different risk profiles. Public companies should avoid merely copying cybersecurity risk factors from others. The SEC will likely deem a boilerplate risk factor too generic and insufficient to inform investors of the company's own cybersecurity risk. If a particular cybersecurity risk factor is applicable to almost any company, then it is likely too generic and should be revised. Instead, companies should disclose the specific facts and circumstances that make a given cybersecurity risk material by taking into account the company's own risk profile (e.g., industry, resources, systems, handling and use of data).

*3. Sufficiently tailor cybersecurity risk factor disclosure to your particular business and industry.*

Cybersecurity risk profiles vary by industry and from company to company within an industry. A public company's risk factor disclosure needs to recognize these differences by clearly explaining in its disclosures the risks or potential types of risks and the likely impact of a breach incident. For example, financial services companies handle large amounts of sensitive client data, the exposure or loss of which could materially harm the business due to a likelihood of customer lawsuits, regulatory enforcement, reputational harm, and loss of clients, among other things. These companies are also at a greater risk of theft of funds from accounts that would have more direct and immediate harm. Contrast this with a public manufacturing company to which theft of intellectual property and interruption of networked or connected operations likely pose significant risks and could lead to interruption in operations, competitive harm, loss of revenues, and costly litigation. In addition, the materiality of certain cybersecurity threats may differ among public companies in the same industry depending on their respective preventative measures, available resources, the experience of personnel, etc. These differences need to be taken into account when drafting effective risk factor disclosures.

*4. Tailor cybersecurity risk factors in light of your company's size and resources.*

Cybersecurity risk profile may vary among public companies depending on size and financial strength of the company, thus reinforcing the need for tailored cybersecurity risk factors. A public company should be careful not to adopt risk factors from the SEC filings of a larger or smaller company in the same industry without proper tailoring. A small or midsize company should not assume that a potential cybersecurity threat disclosed in the filings of a Fortune 100 company in the same industry is also material to the small or midsize company, nor should it assume that an omitted cybersecurity threat in the larger company's filing is somehow not material to the smaller company, and therefore, does not require disclosure. It could be that the board of directors or disclosure committee of the larger company determined that it had adequate safeguards to prevent or minimize a particular cybersecurity threat or that the estimated damages or liability resulting from a cybersecurity breach would not be material. However, that same threat might be material to a smaller company if it is less equipped to prevent the breach, or to withstand any associated financial or reputational loss. Likewise, a large, high-profile company may determine that a particular cybersecurity threat poses a material risk due to the prevalence and frequency of attacks against it, its competitors, or other large or high-profile companies. A smaller company might not (but should be careful not to) view itself as a likely target of cyberattacks because of its lower profile, and/or the lack of publicized cyberattacks affecting similarly situated companies. Certainly, size and resources of the company should be factored into any analysis of materiality.

*5. Give appropriate prominence to cybersecurity within the risk factors section.*

It is common practice to list risk factors in order of importance, thus giving greater prominence to the risk factors that the public company deems most significant. There is a tendency by some companies to add a new risk factor at the end of its existing list or to add to an existing group of risk factors where its placement may seem to be logical (usually related to information technology or systems). However, a company should avoid these tendencies and give careful thought to the relative importance and materiality of cybersecurity risk and then properly position the new or improved cybersecurity risk factor accordingly. We are not suggesting that the cybersecurity risk factor should be automatically placed at the top of the list. Although cybersecurity and the risk of attack is becoming increasingly important to companies of all sizes and in all industries, other risks may still be more significant to a particular public company. For example, it would be understandable if a public company engaged in a heavily regulated industry, such as pharmaceutical sales, gave greater prominence to the risk of a change in law or regulation affecting drug prices or approval processes. Also, a company that has previously been the target of a cyberattack should consider moving its cybersecurity risk factors to a higher position than it otherwise might have in the absence of a prior incident.

*6. Make cybersecurity risk factors understandable to investors.*

It is important to remember that risk factors are meant to help the investor make an informed investment decision. Therefore, they should be written in definite, concrete, everyday language so they are easily understandable. As a general rule, companies should avoid legalese, technical jargon, and business terminology that make the substance of the disclosures difficult to understand. This can be particularly challenging when crafting a cybersecurity risk factor since the na-

ture of the risk does not easily lend itself to using plain English and may require discussion of technical systems and processes that are unfamiliar to many investors. By now, we estimate that most reasonable investors understand terms such as ''malware,'' ''encryption,'' ''firewall,'' ''hacker,'' ''virus,'' and ''phishing,'' but will they understand the meaning of ''IPS,'' ''SSL,'' ''VPN,'' ''social engineering,'' ''keylogger'' and ''pharming''? Thus, public companies must employ careful drafting of complex processes and technical terms to make their risk disclosure understandable.

*7. Review competitors' cybersecurity risk factor disclosures; don't be an outlier.*

Although we earlier cautioned against adopting risk factors from other companies, we see value in periodically reviewing the cybersecurity risk factors of competitors as they can inform a public company of the nature and types of cybersecurity risks that their competitors deem material and which they may want to consider if they have not already done so. Furthermore, if a competitor has been the victim of a known cyberattack, a company might consider this to be material to its investors, perhaps because of the incident itself or the nature of the attack. Public companies should look for changes or updates in a competitor's cybersecurity risk factor disclosures, as these may have been changed in response to an SEC comment. A company may benefit from a competitor's experience and avoid an SEC comment on future filings.

In addition, a public company may wish to consider the scope and robustness of its cybersecurity risk factors in relation to its peers. It seems ill-advised for a company to be an outlier in this regard by providing disclosure that is paltry or even minimally compliant compared with a competitor's disclosures, as this could attract attention from regulators, governance watchdogs, and shareholders. Likewise, companies should consider the degree to which they want to be a leader among their peers in cybersecurity risk disclosure, as ''over-disclosure'' could potentially provide a roadmap to hackers that could ultimately put the company at a competitive disadvantage. Needless to say, a company's relative positioning along the disclosure scale should be carefully considered and constructed so it is meeting the SEC's disclosure expectations regardless of the robustness of a competitor's disclosure.

*8. Avoid exposing vulnerabilities by providing too much information in risk factor disclosure.*

Cybersecurity risk factors are publicly available on the SEC's Electronic Data Gathering, Analysis, and Retrieval database and often on the website of the public company. Thus, companies should strive to meet their cybersecurity disclosure obligations without unwittingly providing a roadmap for would-be cyber criminals to penetrate the company's security protections. The SEC recognizes that this is a real concern and has indicated in its recent guidance that companies are not expected to disclose their system vulnerabilities, potential areas of weakness, or technical information about their cybersecurity systems. Even so, the SEC has made clear that where a company has become aware of a cybersecurity incident or risk, it must appropriately and timely disclose information that is material to investors. Disclosure of such incidents, however, may necessitate more specific or technical discussion of a company's systems, which will require careful drafting.

*9. Involve the right company personnel when drafting cybersecurity risk factors.*

Due to the nature of cybersecurity risk, a public company should engage members of its IT department to work with legal and finance personnel in tailoring its cybersecurity risk factor disclosures. Members of the IT department are likely in the best position to know the company's cybersecurity threat vulnerabilities and preventative measures, and thus, can help draft more accurate and tailored risk factor disclosure. It will be incumbent upon the team to ensure that input from IT members on complex or technical matters is sufficiently reduced to plain English in the final drafting. It is also advisable to involve high-level officers and members of the board of directors having experience in cybersecurity measures and/or the disclosure of these measures as they may bring other perspectives from their experience gained at other companies.

*10. Periodically update ''new and improved'' cybersecurity risk factors.*

The cybersecurity landscape is rapidly changing and so, too, should a public company's measures to prevent and mitigate a cybersecurity incident. Accordingly, the risk factors that a company has crafted may become outdated if not periodically updated to disclose changes in risk profile and the occurrence of new cybersecurity threats and incidents affecting the company and perhaps its vendors, customers, or competitors. Accordingly, we suggest companies assess their existing disclosures as part of their quarterly risk factor review. Smaller companies that are not required to periodically disclose risks should consider voluntary disclosure. A cybersecurity incident can occur unexpectedly and, as risks evolve, it is important for companies to be armed with the proper risk disclosure and to keep their investors well informed of these risks. It should also be noted that public companies have an ongoing duty to correct and update prior disclosures.

## Conclusion

The SEC's latest guidance on cybersecurity puts the issue of cybersecurity risk factor disclosure back in the spotlight following its initial attempt in 2011 to encourage robust risk disclosure. We believe public companies should take seriously this new guidance and take immediate steps to improve the risk factor disclosures in their public filings to meet the standards in the new guidance. Failure to update cybersecurity risk disclosure could have undesirable consequences. By following the steps outlined above and engaging with securities counsel, it is likely that a public company can achieve compliance and mitigate risk.

  PVLR ISSN 1538-3423