The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 1, Number 10 August 12, 2015

SEC

Meeting Expectations for SEC Disclosures of Cybersecurity Risks and Incidents (Part One of Two)

By Amy Terry Sheehan

The SEC has made clear that material cybersecurity risks and incidents should be disclosed to investors. However, determining what is material, as well as when and how to disclose, is less clear. This article, the first in a two-part series, provides guidance on how to make appropriate disclosures that will meet the expectations of the SEC and investors regarding form, substance and timing. The second article will provide suggestions and examples for language to use in disclosures. See also "*The SEC's Updated Cybersecurity Guidance Urges Program Assessments*," The Cybersecurity Law Report, Vol. 1, No. 3 (May 6, 2015).

SEC Guidance on Disclosures

The SEC has become more active on cybersecurity issues in recent years. However, it has not issued updated guidance on the specific issue of disclosures since 2011.

In 2011 the SEC Division of Corporation Finance released guidance regarding disclosure obligations relating to cybersecurity risks and cyber incidents. The guidance remains "the most important piece of substantive interpretation on the topic," Harriet Pearson, a partner at Hogan Lovells, said.

The guidance states that while "no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents." It adds that "[i]n addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading."

"Regulators like the SEC have to find the right balance between encouraging companies to be helpful with investors by accurately and fairly disclosing their risks, and helping sort out what is and what is not material for investors, while not requiring companies to provide a roadmap for hackers as to where they are vulnerable, or requiring disclosures that may trigger lawsuits, but that don't actually add any value," Avi Gesser, a partner at Davis Polk, said.

"Most companies are really trying to get their cybersecurity right. And regulators generally don't want to punish companies that are truly the victims of a cyberattack," Gesser said. "But regulators also want to encourage companies to protect their customer's sensitive data, so if companies don't take cybersecurity seriously, there can be consequences."

Other Guidance

Companies can also review SEC Commissioner Luis A. Aguilar's 2014 speech, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, "about boards and directors and what their role should be in overseeing these types of risks," for guidance about what boards should be looking at, said Kim Phan, counsel at Ballard Spahr. See also "SEC Commissioner Says Public-Private Partnership Is Key to Effective Cybersecurity," The Cybersecurity Law Report, Vol. 1, No. 7 (Jul. 1, 2015).

Companies should also be familiar with the SEC cybersecurity sweep of broker dealers and investment advisers, as that can help predict what type of questions the SEC will ask and what types of documents the SEC will seek in other types of industries, Phan said. See "*SEC Guidance Update Suggests a Three-Step*

Framework for Investment Manager Cybersecurity Programs," The Hedge Fund Law Report, Vol. 8, No. 18 (May 7, 2015).

In addition, the SEC, along with others, has stated that "while you don't have to implement every single step of the [NIST] framework, companies should be assessing to what extent it is in lockstep with that framework and whether or not there are any risks that the company faces that would require it to go beyond the framework or whether the company has potential risk that falls below the framework," Phan said.

Disclosing Cybersecurity Risk

Most, if not all, companies have some level of cybersecurity risk if they have any digital data, network or connected infrastructure. "Information technology and the connectivity it makes possible affects almost every type of business process and operation. Along with the benefits of that capability comes a new type of operational risk that every organization in every industry must contend with by virtue of having digital processes," Pearson said. "It has become very common to proactively include some kind of disclosure about IT, data and/or privacy risks."

She continued, "Some kind of statement describing the risk as it relates to your business makes sense generally because the risk of IT or digital systems and data being compromised is well recognized as being one of the top risks facing businesses." Pearson said. "And if something were to occur where this type of risk manifests in an incident, then you would have appropriately disclosed the risk to your investor community and you can point back and reference the disclosure," Pearson said.

"Cybersecurity is really not that different from any other disclosure issue," Gesser said. "What needs to be disclosed is specific to the company: what it has said previously on this issue, whether it has had a material incident, and the extent to which the company is particularly vulnerable in this area for some reason."

Companies need to go through the process of analyzing their cybersecurity risk and considering whether it has a "different type of inherent risk than other companies," Phan said. This analysis will become "part of the company's risk profile."

How Much Detail to Include When Disclosing Risk?

Too much detail can compromise security. In its 2011 guidance, the SEC acknowledged the downside of providing too much detail, stating, "We are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts – for example, by providing a 'roadmap' for those who seek to infiltrate a registrant's network security – and we emphasize that disclosures of that nature are not required under the federal securities laws."

It is important to "craft a risk disclosure that is appropriately tailored to the nature of the risk as it relates to the company without being too detailed so that it might potentially create a roadmap for interested entities that might have illicit purposes in mind," Pearson said. "Fortunately, high level of detail is not necessary in a reasonable interpretation of the SEC requirements and is probably not wise."

It is also prudent practice to stay in line with the disclosures of similarly situated companies in the same industry because usually companies don't want their disclosures to stand out as lacking in an environment where the SEC may be looking for an enforcement action if a breach does occur, Pearson said. "A company in a certain industry may want to look at other companies in their industry and see what the practice is – how detailed companies are being, what kinds of issues are they bringing up and think carefully how to frame and write the disclosure so that you are not an outlier. If you wanted to be an outlier in terms of having fewer details or more details or different topics emphasized, you should know in advance why you want to do that and do it consciously," she said.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 1, Number 10 August 12, 2015

Disclosing a Cybersecurity Incident

Minor intrusions with no material impact on customer data or the company most likely do not need to be disclosed. Confirmed breaches of customer data or other significant company information, particularly if they trigger notification requirements, should, most likely, be disclosed. For the many incidents that fall in between those two categories, company "management must make a determination whether the possible compromise of customer data may be significant enough to warrant a disclosure and if a reasonable investor needs to know about it, given the totality of circumstances," Pearson said.

If the company is going to disclose the incident, it must also decide the timing, detail and format of the disclosure.

Types of Incidents to Disclose

Experts agree that when there is an incident where customer data is accessed and notification obligations are triggered, the company should disclose that type of incident. But experts agree that there will be small, insignificant intrusions that do not warrant disclosure. One of the most challenging decisions is whether to disclose incidents that fall in the middle of those two clear categories.

"Even companies that do very well in cybersecurity are still hacked from time to time," Gesser said. "But many of those hacks are routine and don't materially affect the company's risk or value."

However, "if a reasonable investor would expect to know about the risks and about the event, that is the fundamental test under existing laws and regulations," Pearson said.

"Anything that is revealed in the news, even if it does not technically require a legal notice to be sent out, that is something that could impact shares, so the shareholders should know, the SEC should know and it should be included in the company's disclosures," Phan said.

The SEC Commissioner stated in his 2014 speech that boards should spend time planning breach responses in advance and that the "plans should include, among other things, whether, and how, the cyber-attack will need to be disclosed internally and externally (both to customers and to investors)." The statement also explained that certain breaches may not "have a direct material adverse impact on the company itself," but impact individuals through the "devastating effects" of the loss of their personal data and that those individuals should be informed about the incident in order to "protect themselves." Commissioner Aguilar emphasized that "[i]n deciding the nature and extent of the disclosures, I would encourage companies to go beyond the impact on the company and to also consider the impact on others."

In addition, companies determining whether an incident is material to investors should consider a wide range of impacts on the company. Besides actual liability – based on what was lost or taken during the incident and the costs associated with providing protections to customers (such as credit monitoring) – it should also consider whether there is reputational harm that will keep customers away, Masterton said.

"Once the company decides that it should or it must disclose an incident to some customers, it should then consider whether a Regulation FD disclosure is necessary to ensure there isn't any selective disclosure of material non-public information," Gesser said. "FD, which stands for fair disclosure, provides that thou shalt not do selective disclosure," Masterton said. "So if some audiences that are potential purchasers have relevant information, the company should disclose anything important to the whole market to level the playing field."

Examining Past Disclosures

The decision to disclose a particular incident is connected to the company's regular disclosures, Gesser said. "It may be that looking back at what the company previously said, some new event, even if it

itself is not material, makes the previous cybersecurity disclosure no longer accurate. In that case, the SEC may expect some kind of update or disclosure."

Gesser added, "If the company has experienced a significant hack, but all the disclosure says is that the company has a risk of possible cyber incidents, that may not be viewed as adequate disclosure." Gesser said.

Nature of the Hack

"Even if the incident itself is not necessarily material, the nature of the hack, the frequency of the hack, the sophistication of the hack, and the person who made the hack may make the company think its risk profile and vulnerability is different than what was previously," Gesser said. "For example if there is a small hack, but it is coming from a sophisticated foreign state actor in likely retaliation against some action by the company – even if the hack didn't do anything, the company may say to itself 'we are being targeted by a highly-motivated and capable group of hackers, our risk profile has changed and we need to update our disclosure.'"

When to Disclose

Experts agree that rushing to disclose an incident is not prudent. The exposure may be ongoing and companies need time to be able to understand, and thus describe, the size and nature of the incident accurately.

"Companies are rightfully cautious about disclosing intrusions because (1) early on, they are worried that they only have partial information, so they are concerned that they will disclose something, and it will turn out to be different or worse; and (2) a lot of these hacks end up being immaterial," Gesser said.

"It requires some forensic analysis; you don't want to disclose too early because you don't have the facts. It is problematic to trickle out information and constantly be correcting information that you have released. So to a certain extent, disclosing immediately is not practical," Phan said.

A company doesn't want to publicly announce there is a breach while it is still vulnerable, Phan said. When the incident is first discovered, the company "doesn't know if it actually left the internal system."

If law enforcement is involved, that could also impact the timing of a disclosure or notification. Law enforcement "may request that a company not publicly announce," Phan said. They may request the company to hold off any disclosure if the hack came from a specific entity or group that law enforcement is tracking, investigating and building a case against, she added.

However, once the facts are gathered, a special filing may be warranted. If there is a notice requirement triggered or a voluntary decision to disclose the incident to the public and/or customers, "then the next question is should there be some sort of an update with the disclosure made to customers. If the event or incident is a significant one or if it is one that a reasonable investor would expect to hear about outside the cycle of the normal disclosure of risk, it is prudent to do a special filing," Pearson said.

A company can also be criticized by regulatory agencies and even Congress for waiting too long to disclose, Phan said. A company does not want to make it look like they "were trying to withhold or hide something."

Level of Detail

"If disclosure is required, sometimes it is better to remain general, at least at the outset," Gesser said. "It is often very hard, especially early on, to really understand what's happening" and the initial reports regarding the timing and duration of the hack, and the number of customer records accessed, will often change. "Companies don't want to be serially disclosing information. Once you've disclosed at a certain level of detail, you may be expected to continue reporting at that level of detail, and then you may need to update many times."

If certain types of information are affected, such as health-related PII under HIPPA, specific content requirements for notices may be dictated by the

relevant laws. In those cases, the same level of detail should be disclosed to the SEC, Phan said. "Generally those types of disclosure requirements include: the nature of the breach, the number of people impacted, the categories of data involved, the company's remediation and actions to prevent future breaches, and credit monitoring or other corrective action the company is providing to those impacted individuals. Those are the kinds of basic information most people would want to know and the SEC would expect to know."

Form of Disclosure

In the wake of a material incident, companies should issue a supplemental disclosure right away, Joseph Masterson, a partner at Quarles & Brady, said. "The minimum responsibility is the annual obligation to disclose in the 10-K material information about special risks and then to update that information quarterly if it's changed," Masterson said. "If there is a major breach, they file an 8-K special report and not wait for the next cycle the way they would normally do it with an SEC filing."

In other circumstances, the nature of the incident may not require an immediate supplemental disclosure, and the company may decide to instead include updated language in the next scheduled disclosure.

In addition, notes to the financial statements should include a management discussion and analysis of the cyber program, Masterton said.

Website Updates

"Having some amount of information available on the website is increasingly common. It is an easily updatable place to provide real-time information to those who are interested about a breach," Phan said. "There is the physical letter that goes out, but that is a static one-time notification that can provide a website where someone can go and regularly check developments. A lot of the letters are generically-phrased and can provide a website to check whether one's information was actually hacked, and if it was, what types of data might have been involved. Although physical letters are not going away anytime soon, the heightened functionality available online may become increasingly favored by consumers and regulators over time instead of just a vague letter."

Documenting the Disclosure Vetting Process

It is a good practice for companies to have backup for each risk disclosure, and that should include cyber-related disclosures, Pearson said. "There is a fair amount of back and forth going on between companies and the SEC around cyber-related disclosures. So if there is a follow-up question from the SEC, having done some work in advance to be ready to explain why the risk factor was written that way and why other disclosures were made is a prudent step to take," she said.

Documenting the process that the disclosure committee, or the committee by another name that tackles this task, undertakes to determine whether to disclose something (i.e., the types of events brought to the committee, how the committee was set up, how decisions were made) is valuable in advance of a potential inquiry, Pearson said.

SEC Enforcement

While the SEC has not brought an enforcement action yet, they have been sending questionnaires and comment letters to learn more about companies' reasoning. Experts agree: if the SEC finds in the wake of an incident that a company had been misleading about its cybersecurity risks and/or the incident itself, the SEC will use its enforcement power.

Disclosing Third-Party Breaches

"One of the problem areas that the SEC and other regulators are starting to focus on is breaches with vendors," Phan said. "While companies may be reporting their own incidents and their own risk profile and talking about their own breaches, there is increasing pressure for there to be downstream disclosure as well. A company is using many vendors – does it know if they

have had breaches and if any of the breaches impacted its own data? Downstream disclosure is something the SEC is going to be increasingly interested in."

Role of the Board

"Boards are responsible for the filing, they are the ones that the SEC will come after, but increasingly they are also at risk of being held accountable otherwise – directly by shareholders and derivatives suits," Phan said. "After a breach, shareholders are looking to the board and asking why weren't you on top of this? Boards are at risk from multiple fronts at this point. When the company discloses something in the SEC filing, the shareholders see it and may file a lawsuit against the board."

The SEC Commissioner also emphasized the board's role. "[E]nsuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's oversight responsibility . . . [B]oards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril," he said.