SEC's Cybersecurity Disclosure Rules Are Here. Is Your Company Ready to Comply?
Sam Gandhi, Sonia Gupta Barros, and Colleen Theresa Brown
September 2023

Sam Gandhi:
Companies are facing more tax on their information systems, and as their cyber risks skyrocket, the SEC has stepped in with new regulations telling businesses what to disclose about these incidents and possibly even how to manage them. With the deadline for compliance fast approaching, businesses are scrambling to mitigate their legal risk and comply with new SEC regulations that some say may be an overreach.

Sonia Gupta Barros:
Companies should really take compliance seriously. The SEC's Division of Enforcement, they have a dedicated cyber unit, and just last year, they allocated a number of additional positions to that unit.

Sam Gandhi:
That's Sonia Barros, a partner in Sidley's Capital Markets group and Co-Lead of its Public Companies practice.

Colleen Theresa Brown:
But I think a lot of people are concerned about the litigation risk here and the Monday morning quarterbacking, asking the question of what the company knew or should've known, at what time, at what point in the incident response process?

Sam Gandhi:
And that's Colleen Theresa Brown, a partner in the firm's practices in Privacy and Cybersecurity, Commercial Litigation and Disputes, Crisis Management and Strategic Response, and Insurance. In today's podcast, we're going to discuss the SEC's newly-adopted regulations for disclosing information on cyber risk and how companies and their boards can best apply.

From the international law firm Sidley Austin, this is *The Sidley Podcast*, where we tackle cutting-edge issues in the law and put them in perspective for businesspeople today. I'm Sam Gandhi. Hello, and welcome to this edition of *The Sidley Podcast*, Episode number 35. Sonia, Colleen, it's great to have you on the podcast today.

Sonia Gupta Barros:
Thank you, Sam. Great to be here.

Colleen Theresa Brown:
My pleasure. Thank you for having me.

Sam Gandhi:
This summer, the Securities and Exchange Commission adopted rules for companies disclosing key information regarding cyber risk. The rules, which took effect September 5, focus on public companies providing transparency to investors through formal disclosures. Not everyone's happy with the new rules.

A group of Republican lawmakers recently sent a letter to SEC Chair Gary Gensler contending the rules will create more bureaucracy and more risk, compromising the confidentiality of public companies. "It is unfathomable that the SEC is moving forward with its public disclosure requirements which will only increase cybersecurity risk," the letter said.

So, Sonia, let me start with you, and give us the lay of the land, and talk us through the background of how these rules were adopted.

Sonia Gupta Barros:
The SEC has really long been concerned about cybersecurity risk and how companies inform investors in the markets about those risks. Back in 2011, the Division of Corporation Finance had issued interpretative guidance on the types of cyber disclosures public companies should be providing.

These were not new rules, but what the SEC said is that, under the SEC's existing rules — risk factors, MD&A, business description, legal proceedings — companies should be providing full-service disclosure on material cyber risks, and the SEC also emphasized that companies should

consider reporting material cyber incidents on Form 8-K, where it makes sense to do that.

Then, in 2018, the commission actually affirmed this SEC staff guidance and added that companies should also consider any insider trading concerns and add disclosure on board risk oversight, and at that time, that's when most companies started including something in their proxy statement on board risk oversight with respect to cyber. So, fast-forward to this year. In essence, the SEC believed that material cyber incidents were being underreported and that the existing reporting requirements were not providing investors with timely information.

In the adoption release for the new cyber rules, the SEC noted that, in 2022, for domestic U.S. public companies, there were only 35 Form 8-Ks that were filed reporting material cyber incidents, and for foreign private insurers, 22 Form 6-Ks. So, basically, the SEC believed that investors needed more consistent disclosures about cyber incidents and more information on a company's cyber risk profile.

So, that's why, this year, the SEC adopted these new rules with respect to cyber incident reporting and a company's cyber risk profile. In essence, the new requirements include both Form 10-K disclosures and a new item on Form 8-K. The new rules are fairly extensive. They require new disclosures on a company's cyber risk management strategy and governance.

It's really an unprecedented level of disclosure into how a company manages its cyber risks. It also requires public companies to report on 8-K or 6-K for a foreign private issuer when they have a material cyber incident that's determined without an unreasonable delay, and this can really pose a significant challenge to companies determining when the incident becomes material when they're in the midst of responding to an active incident.

Sam Gandhi:
Colleen, obviously, not everyone is satisfied with the finalized requirements issued by the SEC. So, what are the pain points? Sonia just mentioned one of them, but what are the others?

Colleen Theresa Brown:

The final rules were approved in a 3 to 2 vote, and this was following a lot of comments submitted by the industry, raising concerns that, in part or taken into consideration…and we see changes reflected in the final rule, but a lot of the concerns were ultimately not acted on, and we see some of the most significant concerns reiterated again in the dissents.

So, that 3 to 2 vote, we have two very strong dissents from Commissioner Peirce and Commissioner Uyeda. Commissioner Peirce discussed how these final rules take an expansive view of the SEC's authority and raise concerns that these rules may, in effect, lead to SEC micromanagement of cybersecurity programs and concerns that these final rules may muddy the determinations that public companies have to make on materiality by expressly rejecting financial materiality as the cornerstone consideration when it comes to a cybersecurity incident.

The dissents note how it will continue to potentially put registrants at heightened cybersecurity risk in the middle of responding to an incident by giving threat actors insight into the incident response process. This concern about those immediate early hours of incident response is heightened by the timeline requirement to issue something within four days of determining that an incident is material, where a company will have to speak about an incident when it may not yet be contained.

Dissents also highlight non-material risk management and governance disclosures and concerns how an overly narrow law enforcement exception doesn't defer to other government agencies with overarching mandates to protect national security, public safety, critical infrastructure. Another good point made by Commissioner Uyeda noted that, and I'll quote him, because I think it's worth reiterating: "Rather than using a scalpel to fine-tune the principles-based approach of the 2018 Interpretive Release, today's amendments swing a hammer at the current regime and create new disclosure obligations for cybersecurity matters that do not exist for any other topic."

As we know, there's a lot of key areas of risk that are dealt with in 10-Ks and for which companies may need to issue, you know, an 8-K on, but as Sonia said, it's really an unprecedented level of disclosure specific to cybersecurity risk.

Sam Gandhi:
Colleen, let me just follow up on one thing that you said in terms of the law enforcement narrow exception. Does that mean that if the National Security Council, or any other type of federal agency, basically told the company not to disclose this, the company would find itself between a rock and a hard place?

Colleen Theresa Brown:
In effect, yes. However, there is an expectation that there will be coordination internally between agencies so that if there is an incident that truly does present a risk to public safety or national security, that the relevant company would be able to get a reprieve, a 30-day reprieve. This exemption exception is in the rules for the attorney general of the United States to essentially confirm that disclosure can be delayed for those reasons.

But there's certainly a lot of anxiety around that process, what that process will be, and how it will have to play out in a very short timeline. Within four days of determining a cybersecurity incident is material, the company will have to make that disclosure, unless they get that reprieve, and the details of how a company will go about doing that are not yet set.

Sam Gandhi:
Sonia, let's get into the substance of these rules. If I'm a key stakeholder at the company, what are my main areas of concern?

Sonia Gupta Barros:
You definitely need to understand the new requirements, and there's a lot of detail here, so I think it's very important that companies and key stakeholders within the company understand it, right? There's the new 10-K or Form 20-F requirement, and then there's also the new Form 8-K incident reporting requirement, 6-K for foreign private issuers where relevant, and so, for the annual report 10-K requirement, there's basically four parts to the new disclosure.

First, there's detailed disclosure on a company's processes that they have for monitoring and managing cyber risks. Second, is disclosure on actual risks for cybersecurity threats, and this one is interesting, because most companies already provide disclosure on material cyber risks and their risk

factors, but here, the SEC felt that these disclosures were not sufficiently prominent and that they were often buried in with other unrelated disclosures.

So, they wanted to see cyber risk disclosures highlighted in this new section of the 10-K. A lot of this may be a repeat for some companies, but they'll certainly need to revisit their existing risk disclosures. The third piece is board oversight of risk from cybersecurity threats. For this requirement, it's important for companies to note there's no materiality qualifier here. The SEC said if a company has determined that a board oversees a particular risk, that fact, in and of itself, is material to investors.

Now, the good news about this is most companies already have something in their proxy statement about board risk oversight pursuant to the 2018 guidance. So, companies may be able to draw on that, but they should be thinking about this in light of the new requirement. And then, lastly, the fourth 10-K requirement, the fourth component, is disclosure on management's role in assessing and managing material cybersecurity risks.

And this will require detailed disclosure on management positions and committees responsible for cyber risk oversight within a company. For many companies, this is going to be a new disclosure. Certainly, they may have the processes in place already, but it will require companies to think about what those processes are, collect information on them, and then describe them in a succinct fashion, and then also to include a description of how information is communicated to the board.

Then, there's also the 8-K requirement, right, on material cyber incidents, which has to be reported within four business days of determining if the incident is material, without unreasonable delay, and those terms, without unreasonable delay, are not defined by the SEC. So, it's subject to Monday morning quarterbacking and interpretation down the road by plaintiffs' attorneys and perhaps even SEC's Division of Enforcement.

And companies in the 8-K will need to describe the material aspects of the nature, scope, and timing of the incident and also the material impact, or reasonably likely material impact, and as Colleen mentioned, the exception for a delay in reporting is very limited. It's only if the U.S. Attorney General

determines that there's substantial risk to national security or public safety, and then notifies the SEC in writing.

Sam Gandhi:
Colleen, based on what was originally proposed by the SEC in 2022, how do the adoptive requirements differ, and what are the significant changes?

Colleen Theresa Brown:
I want to start this by reminding everybody about a key point, Sam, which is the legal standards for materiality have not changed, and so, a lot of what we're wrestling with in these final rules, they're not new. Companies have had to consider materiality and material risks and disclose material risks for a long time.

Companies have had to consider whether a data breach might be material and whether it should issue an 8-K for a long time, as well, and the law underlying, making that materiality determination, has not changed. And that's really important to emphasize because, one, I think it can help people take a deep breath about this and go back to the basics, right, back to the principles here.

But also, it highlights, at the same time, that if there are significant changes you make to your program here, hindsight's 20/20, and because the legal standard has not changed, there could be some hindsight and litigation risk with respect to past incidents around this, as well. So, I think a moment of caution and a deep breath to remember that we're still back to the basics.

Now, also, another piece of good news is there was some narrowing of the final rules based on the thoughtful comments, many, many thoughtful comments, that were submitted in this rulemaking process, and one of the most important changes in the final rule from the proposal is that the information that needed to be included about a cybersecurity incident was narrowed from the proposal, the information required.

And so, that goes, in part, to address the concerns that the 8-K could expose a company further, in the midst of battling and containing a cyber incident, and so, some of the most concerning points were pulled back. The other point is the attorney general delay in reporting. I mean, there were

clarifications in that. I think there still are concerns, and a lot remains to be seen on how this will be operationalized.

I think a lot of people are hopeful that there will be some reasonable processes to address those concerns. Another thing that was added in the final rules was an exception for breaches of CP&I subject to the FCC breach reporting rule. That's customer proprietary network information and the telecommunications industry-specific regulation. Of course, a lot of people are disappointed that the SEC did not recognize other legal regimes in other industries that set standards for reporting data security incidents.

For example, HIPAA. The SEC said there was no conflict there, and so, they only put an exception in place for CP&I, but that was a change, and then there was an important clarification. A lot of people were concerned about language in the proposed rules that was backwards looking about past incidents and the cumulative effects of past incidents that companies would have to consider and potentially issue disclosures, and the SEC clarified there that that relates to related data security incidents.

So, if there's a series of smaller, non-material incidents that are related, that, together, present a material risk, then that could trigger an 8-K. So, those were important clarifications, and there was also on the other side of the rules, on the 10-K, on the risk management and strategy governance side, there were some changes that were certainly welcome, including less granular required disclosures around risk management strategy.

There was the removal of certain required descriptions that had been proposed for how a board integrates cybersecurity into business strategy and risk management and financial oversight. Another thing that a lot of directors were really focused on, they did remove a proposal to require disclosure of cyber expertise on boards, I think in recognition of the reality of the composition of boards and also in recognition, in large part, that cybersecurity is an enterprise-level risk worthy of attention by everyone on the board.

So, there were some definite important revisions in the final rule that were in recognition of some of the comments that were submitted in the process.

Sam Gandhi:

You're listening to *The Sidley Podcast*, and we're speaking with Sidley partner Sonia Gupta Barros and Colleen Theresa Brown about the new rules regarding how to disclose cyber breaches to investors. So, Sonia, as I understand it, companies are going to need to be in compliance with this regulation by December of this year. Since we're sitting in mid-September here, that seems a little tough. What are you hearing from clients, and are most companies hitting the ground running?

Sonia Gupta Barros:
The first thing that companies need to do is pull together their relevant teams and have discussions about getting ready to comply, and this isn't so simple because it could include people from various parts of the organization. Certainly, it's going to include IT personnel, also folks from the legal department, SEC reporting, perhaps even compliance, and risk enterprise. So, that's a lot of folks to get together. You know, Colleen and I frequently participate in calls with clients.

And there is typically a good, sizeable number of folks from different groups, and once you have the team together, then there are various steps you need to go through. The first is really understanding the new requirements and concepts in the rules, because these go beyond what historical reporting has been for cybersecurity risks and incident reporting, and so, it's really important that companies and the key stakeholders within the company understand the rule.

There's a nice summary chart that the SEC has on page 12 of the adopting release, if companies want to refer to that, and of course, Sidley has a summary that's comprehensive, as well. Once you've done that, then companies and their IT personnel and other relevant people should update their internal incident response plans and any other processes, and that really just depends on what processes the company currently has in place.

They may need to change certain lines of communication, even certain reporting lines if needed, and this is all to ensure that the company can make a timely determination on materiality, right, without unreasonable delay within four business days, and that they can continue to evaluate materiality throughout and beyond the life cycle of the incident response.

So, that's with respect to the 8-K. For the 10-K disclosures, the company should carefully review their existing cybersecurity risk management strategy and governance, and they should go ahead and start drafting the new disclosure for the 10-K, because for calendar year-end companies, this is going to be in the 2023 10-K filed in early 2024.

And once they get that draft of the 10-K disclosure done, then they can decide if they want to make tweaks to any of their processes behind the scenes so that that can be reflected in the new disclosure, and then, lastly, as I briefly mentioned, because there's a new, discrete requirement on cyber risk disclosure, companies should revisit their cyber risk factors and think about how to pull out and consolidate that disclosure in a new section.

Sam Gandhi:
As a follow-up for you, Colleen, what's been your experience thus far regarding the reception of clients to the rules, and what are clients telling you?

Colleen Theresa Brown:
Certainly. Well, it is getting a lot of attention. I'll say that. Sonia and I have done many, many, many client calls with a variety of stakeholders, and there's a few things, I'd say, people are really focused on. One goes back to the timeline of the four-day reporting. It causes concern.

People, I think, really recognize that there's a variety of data security incidents. No one is exactly the same, and there may be some material incidents that it's very easy to understand that the clock has started ticking from the very discovery of an incident. Occasionally, that happens, but very often, a data security incident starts smaller.

And it takes time to investigate pulling the threads of an incident before you fully understand the scope, and I think a lot of people are concerned about the litigation risk here and the Monday morning quarterbacking, asking the question of what the company knew or should've known, at what time, at what point in the incident response process, and matching that up to the four-day timeline.

So, in response, a lot of companies are taking a look at the incident response plan. Doesn't necessarily mean that it needs to be updated. A lot

of incident response plans are quite good as they are and have long anticipated the need to consider materiality determinations, but there certainly are some clients and companies who've decided that there could be some updates to the documentation there, and again, practicing for muscle memory, making these determinations, which usually involve a lot of different stakeholders within the company.

So, tabletop exercises, you know, that is always a best practice that companies have been doing for quite a long time, but tabletops that expressly contemplate a material incident so people can practice that and other cyber incident prep, ensuring that people are happy with what they can say about the program in their 10-K, and part of this is in response to board questions. The boards are very interested in these proposed rules and in the final rules, as well, and the renewed activity around board-level tabletops has certainly been very hot right now.

There's also a lot of consideration about third-party risk assessments. People talking about NIST benchmarking, and just generally, again, going back to the basics of cyber risk management. Of course, a lot of people are talking about their concerns that the rules might do more to enhance the security litigations frequency than actually improving cyber risk management and oversight.

A lot of concern that the rules are not harmonized with other mature cybersecurity regulatory regimes, which complicates incident response. But at the end of the day, all of these questions and these conversations are focused on cyber risk oversight and management, which, you know, hopefully will be a good thing at the end of the day. More people focused on this important enterprise risk.

Sam Gandhi:
Sonia, what's on the horizon, and as we look to the future with regard to cybersecurity, what should clients know?

Sonia Gupta Barros:
Companies should really take compliance seriously. The SEC's Division of Enforcement, they have a dedicated cyber unit, and just last year, they allocated a number of additional positions to that unit. We had also seen a number of enforcement cases that the division brought in the last few

years, as well. So, they should definitely take compliance very seriously. The SEC also plans to adopt additional cybersecurity rules applicable beyond public companies.

So, later this year or early 2024, the SEC is expected to finalize proposed rules on cybersecurity regulations for registered investment advisers, funds, and broker dealers, and they're also looking at significantly amending rules for customer information that's protected under Regulation S-P and for entities operating systems that support key market and trading functions under Regulation SCI.

Sam Gandhi:
Sonia, let me follow up with one thing. Do you see the rules as enhancing the greater risk of shareholder litigation against companies?

Sonia Gupta Barros:
Yes, Sam. Definitely. Anytime you have more detailed rules, you can expect to see an increase in shareholder litigation, and here particularly, where there's an opportunity to, with the benefit of hindsight, judge a company's determination of materiality. I think that will certainly lead to more shareholder litigation after the fact.

Colleen Theresa Brown:
I agree with that, and I would add that even broader than shareholder-related and SEC-related litigation is the broader risk of litigation around cybersecurity, and the more you say, just broadly, about your program, the more that could be used in other kinds of disputes, including class action litigation.

It's also a good reminder that the SEC, for a long time, has been emerging as one of the strongest cyber regulators on a variety of contexts, but they're not the only ones. They're not the only cyber cops on the beat. There is a variety of regulators that are enforcing and are active in investigating cybersecurity incidents and cyber risk management, both in the U.S. as well as globally, and so, the scrutiny on companies' cybersecurity programs has never been higher.

Sam Gandhi:

We've been speaking with Sidley Partners Sonia Gupta Barros and Colleen Theresa Brown about the new rules regarding disclosures of cybersecurity events and what businesses can do to mitigate their legal risk. Sonia, Colleen, this has been a great look at the landscape regarding SEC's new regulations, and thanks for sharing your insights on the podcast.

Sonia Gupta Barros:
Thank you, Sam.

Colleen Theresa Brown:
My pleasure. Thank you for having me.

Sam Gandhi:
You've been listening to *The Sidley Podcast*. I'm Sam Gandhi. Our executive producer is John Metaxas, and our managing editor is Karen Tucker. Listen to more episodes at Sidley.com/SidleyPodcast, and subscribe on Apple Podcasts or wherever you get your podcasts.