TheCorporateCounsel.net Providing practical guidance for over 40 years.

"The SEC's New Cybersecurity Guidance"

Wednesday, March 14, 2018

Audio Archive

With the SEC's new cybersecurity guidance here, there are a number of wide-ranging things for you to consider now. Join our experts - all of whom are former senior Corp Fin Staffers:

- **Meredith Cross**, Partner, WilmerHale LLP
- **Keith Higgins**, Partner, Ropes & Gray LLP
- **Dave Lynn**, Editor, TheCorporateCounsel.net and Partner, Jenner & Block LLP

Dave Lynn, *Editor, TheCorporateCounsel.net*: Hello everyone. This is Dave Lynn, Editor of TheCorporateCounsel.net and I'm partner at Jenner & Block.

Welcome to today's webcast, "The SEC's New Cybersecurity Guidance." I'd like to introduce the great panel we have, both of whom were former Directors of the Division of Corporation Finance that had to grapple with the topic of cyber security disclosures in one way or another. Meredith Cross, a Partner at WilmerHale LLP and Keith Higgins, a Partner at Ropes & Gray LLP. Thank you both for joining us.

Why This Topic?

I think the way to start this off is why are we always talking about this topic? That's how if we look at the question I ask myself when I find myself at these types of programs. Obviously, the interest in this topic ebbs and flows a bit with the attention that's raised by cyber breaches which impacts the public consciousness of how well companies are securing personal identifying information and other types of information that they hold near and dear.

That public perception obviously creates a lot of pressure on lawmakers and policymakers and often prompts them to react.

I often point out, we have a disclosure regime that becomes a default mechanism by which to get at the conduct of large companies of all shapes and sizes - because there's really no conduct regulation of large companies.

You have regulated entities obviously who might be in a particular industry that's regulated by a federal government agency but across the board on a topic like cyber security disclosure, we don't have a framework that says, "You must have these types of procedures in place to protect yourself against cyber security breaches."

The logical lever that people tend to reach for is the public disclosure regime which is interim factors obviously as oppose to as a policy tool, but that hasn't stopped anybody before from using it as such.

I think a convenient way to show progress in this area, apps and wide-ranging legislation that would compel public companies to do something in this realm is to have them talk more about it and ensure that the disclosures they're making more about it are fulsome enough that people understand that actions have been taken whether before breach or after breach to try to address the situation as expeditiously as possible.

That's why we keep coming back to this topic as we'll talk about today. We're talking about the disclosure concept that's spent over seven years now in terms of how to approach this type of issue and deal with it going forward.

We're focused today on the new guidance that came out in February. The SEC's release that was a statement and interpretive guidance on the topic of cyber security disclosure. First off, the release itself - it's probably worth noting what it's not. It's not a proposal to change any roles.

There's nothing in there that seeks notice & comment or in the style of disclosure. The release asks questions about what to do in this realm and in many ways, as we'll talk about throughout the webcast, it's not a significant departure from where we've been to date regarding cyber security disclosures over the past seven years.

As many of you are aware in October of 2011, the Staff of the Division of Corporation Finance published "CF Disclosure Guidance Topic No. 2, Cyber Security." I'm going to refer to that guidance as Topic 2 or the 2011 Guidance. I'm sure my panelists will probably shorthand it that way too since that title is a mouthful.

What was noted specifically in the Commission's latest statement is that they were reinforcing and expanding on the Staff's 2011 Guidance - and in that expansion, category addressing topics that were not addressed directly in the October 2011 guidance.

They were touched up in some ways at least in one case. And that's the importance of policies & procedures that companies have around cyber securities and cyber securities issues - including disclosure controls & procedures - as well as the application of insider-trading prohibitions in the cyber security context which wasn't an issue that was really talked about in the 2011 Guidance.

In this latest statement, the Commission says they're continuing to consider other means of promoting appropriate disclosure of cyber incidents. One might read that perhaps as they would consider rulemaking in this area - whether that might be in the form of current disclosure or additional line items disclosure for periodic reports.

That is something that remains to be seen. We haven't gotten any indications that type of thing is on the horizon, but nonetheless it was noted that they're continuing to look at it.

Also, in the release, it was noted that the Staff in its filing review process will continue to monitor cyber security disclosures carefully. In that regard, also in the Chair's statement and interpretive guidance, Chair Clayton basically said, "I've directed the Staff to look at the disclosures and continue to monitor them" - which they have been doing really for a long time now.

Going back to the 2011 Guidance, obviously, it's probably important to note that it's not just Corp Fin's interest, there's also been Enforcement interest. I think everybody understands that this is not just for the issues around disclosure of cyber security generally, but particularly in situations where breaches have occurred.

Back in October, Co-Enforcement Director Stephanie Avakian noted - and expressed her own views - that while to date there haven't been any enforcement actions brought around disclosure failures in the cyber security space, she can certainly envision a case where enforcement action would be appropriate - but she acknowledged that this is a complex area and involves significant judgment. That they're not looking to second guess reasonable good faith disclosure decisions. Against that backdrop, we can look at this new SEC statement.

Meredith, what was the context in which 2011 Guidance came about when you were Director of Corp Fin and how did the Staff approach it at that time?

Meredith Cross, *Partner, WilmerHale LLP*: That's a good summary of where things are now. Back in the day in 2011, cyber security was a huge concern. It was new. The breaches were just starting to becoming bigger and presented more risk to the public.

It wasn't necessarily investor-focused. The federal government, at the time, was considering imposing standards for cyber security across companies having nothing to do with a disclosure approach.

At the same time that was happening, there was some interest on Capitol Hill in doing a bill on cyber security that would have addressed both disclosure and what you had to have in terms of cyber security.

I and several other people from the Staff had meetings with people on the Hill about the fact that the Commission's current rules already were set up to address cyber security disclosure requirements.

There was no need for legislation or additional disclosure requirements to require better disclosure about this particular topic. We wanted to make sure people understood what the potential sources of disclosure obligations would be under the current rules.

That was the backdrop at the time in 2011 for that guidance and, in many ways, was similar to what the new Commission statement does. It went through all the different ways that there could be disclosure required, listed them out and gave some guidance about how to do that.

I personally was very worried about pushing for too much disclosure. The 2011 guidance does say a couple of times that you don't have to give a roadmap. I was pleased to see that showed back up in the new Commission release.

One thing that is an interesting comparison as you're looking at this topic is that going way back in time when the Year 2000 was a big concern and whether public companies were prepared for it. The Staff did put out interpretive guidance about how to make Year 2000 disclosure. I wasn't working at the SEC at the time.

Keith Higgins, *Partner, Ropes & Gray LLP, Partner*: Thank goodness they did, right Meredith?

Cross: When there wasn't enough disclosure in response to the staff Y2K guidance, the Commission put out a Y2K interpretive release to elevate the topic. That's what the new cyber release does. It elevates the topic since Commission level guidance is stronger than Staff level guidance. That's meaningful. I think that's the perspective I can give.

Disclosures Going Forward

Lynn: That leads us to the obvious question - what should we do now that we have this new guidance?

It came out after many large companies have already filed their 10-Ks - but before many companies filed their proxy statement. It has some wide-ranging discussion of the line items that make up the

disclosure that you have in your 10-Ks, 10-Qs and proxy statements. It also talks in some detail about the nature of current disclosure around these types of topics. Our first question is - where do we go from here? Are we back to the drawing board for our disclosures?

Cross: My reaction first off is, "no, we're not." As you noted David, the 10-Ks were essentially all locked down by the time the guidance came out. I had been concerned that if there was something dramatically different in the guidance, people would have to unlock them, even if they're ready to file, to add require information.

I didn't see anything in the guidance that meant you couldn't just file the 10-Ks that were ready to go anyway. I think people really expect as far as the line items go to look at the 10-Qs and next year's 10-K as the place to deal with the new Commission guidance.

The one thing for proxy statements the guidance says that you should think about what to say about the board's role in overseeing cyber security risks. It talks about board oversight of risk.

I have suggested to clients that they look at the disclosures they have. If there's something that fits to add to indicate where cyber is overseen - which committee, for example - that could be something worth adding.

I think eventually companies are going to add more extensive information about that. I would think that will end up being next year after there's been time to think about it at the board level, talk about it - and reflect that discussion & analysis in disclosures.

I'm not sure it makes sense to talk at length about how you oversee cyber risk as compared to any other material risk. I don't think people talk extensively about how the board oversees any particular risk.

That is something that will evolve over the course of the year. One thing is that if you have a board member who has some cyber skills that were relevant to you in selecting that board member - or are now helpful to you - that might be something you want to highlight. I don't think this should result at this point in any significant changes to your proxy statement.

On the other disclosures, I'd say that the area where the Staff is going to be looking at this disclosure, particularly for companies that have had incidents or do business with companies that have had incidents, looking at your risk factors and making sure that they're not hypothetical when things are actually happening. That's been the case already.

It's worth looking again to make sure that it doesn't happen again. Corp Fin Staffers do Internet searches and see if you already had breaches - and then if you did, they would raise that as a comment.

In other areas where I could see the Staff raising comments - based on the new guidance - would be perhaps adding some additional disclosures to MD&A for risks, trends & uncertainties for costs of cyber protection if that's becoming more material for your company.

That could be a trend that I see them saying, "Why aren't you addressing that? Aren't you spending more money on it? You're saying in risk factors that you may have to spend more money on it. Are you spending more money on it as a percentage?"

Also, if you have had a breach and in the risk factor you talk about things that could happen, I could see the Staff raising questions about your MD&A and are those things happening? Are those trends, events or uncertainties requiring disclosure in MD&A? Those are areas I would take an especially careful new look at.

Higgins: I think that's right. I continue to believe that - at least for your business and financial information - if you've been following the 2011 Guidance, there probably isn't much you should be doing. Although I think it's probably a good idea to take a fresh look and make some changes to the disclosure, so you will have done so.

Lynn: Yes, that makes sense. I would say the guidance - in addition to the comments that people generally got which augmented the guidance to some degree and some of those concepts like the one Meredith mentioned – is about making sure you are talking about things that happened rather than just hypothetically.

Timing of Disclosures

I guess one of the bigger differences between this release and the 2011 Guidance, Keith, was this notion of how is the current reporting supposed to go? That's probably worth delving into, because they made several statements in the release encouraging timely current reporting of that.

Higgins: I think the good news on that front is that the Commission didn't attempt to create a new duty to disclose out of thin air. I think they tried to recognize and talk about current reports. They made clear that it was to maintain the accuracy and completeness of disclosures that you would file an amendment to do that.

They talked about when you become aware of the material cyber security incident, you're expecting to make timely disclosure before offering and selling securities or before your insiders trade in those securities.

Again, I'm not suggesting that there was some immediate reason that a company had to make disclosure when between quarters it found itself investigating something that wasn't a cyber security incident.

It then discussed the duty to correct – obviously, if you've made a false statement you subsequently learn is false, you need to correct it.

They pushed into the so-called 'duty to update' - which reading through their release, I had to chuckle, because they had an internal debate going on within the footnote about whether in fact, there is a duty to update. Whether in fact any of the disclosures you make are intended to have a continuing effect.

My advice is to look at the disclosures and make sure your disclosures don't have any implications that can be relied upon other than as statements of fact as they exist at the current time. Dave, Meredith any thoughts on that?

Cross: I think several of us who don't think there's a duty to update unless you've really done something to create one were surprised by the language in the release, but then as you mentioned, chuckled at the internal debate within the footnote that says, "there is no duty to update."

I don't think this is different from any other topic. If you put information out - and it was wrong when you put it out - then you must consider correcting it if it was material.

If you put information out and you're not otherwise speaking and have no other obligation to speak, you likely don't have to update it at random times. You do have to see what else is going on at the time, who otherwise is buying back securities or doing something else. You may have to do something.

I don't know David if you think differently. I don't think they intended to create a duty to update for cyber disclosures.

Higgins: They probably liked to, but I don't think they intended to.

Cross: I'm not sure if they is "everybody."

Higgins: Yes, that's true. Let me say, some would like to. Go ahead Dave.

Lynn: One thing I noted in the separate statement that Commissioner Stein made - she noted her disappointment with the release, because it didn't go far enough in a number of respects. One of which was "we didn't take an opportunity to propose or seek comment on adding an S-K item about cyber security." I think part of this release was pushing the current disclosure notion as far as they could without turning the guidance into "de facto" rulemaking.

Higgins: To a point Meredith made earlier on timing of disclosures, the Commission was good in recognizing that people need to collect all the material facts before they put the disclosure out.

Although they did go on to say that the fact that there's an ongoing internal investigation or law enforcement investigation, that is not a reason that you're entitled to not disclose anything that would otherwise be material and required to be disclosed.

That is no different than the situation where we find ourselves in now. Dave, should we talk about disclosure controls & procedures?

Lynn: Yes, definitely.

Disclosure Controls & Procedures

Higgins: One of the things this release talks a fair amount about is something that has been around since Sarbanes-Oxley. Most companies have detailed disclosure controls and procedures. In my experience, they focus on periodic disclosure - but also to some extent on event-driven disclosures.

In the 2011 guidance, there was mention of disclosure controls and procedures and how they should be considered in the cyber security context. Although interestingly, the examples that were given related to information systems that affected the way the company processed information that it used to prepare it's reports as oppose to disclosure controls. A cyber incident itself needed to be disclosed as an incident.

Cross: Yes, at the time the thought was if your disclosure controls and procedures wouldn't work right because you have been breached, then you have a problem - which I think is certainly still the case.

Higgins: Absolutely.

Cross: This is going to a different point.

Higgins: Yes, one of the hardest things about event-driven disclosure controls and procedures is that you could write all you want about it, but at the end of the day what you need is someone getting the information who is familiar with the requirements under the securities laws and what needs to be disclosed.

Specifically on cyber disclosures, most companies have a relatively detailed list. Most companies that are well-managed have thought about this - and have cyber incident escalation paths and procedures that are used for IT and technologists to be able to assess what's happening at the company.

Somewhere that dissemination of information to the appropriate people needs to make a bridge to the people who are familiar with the securities laws. One thing that you always need to protect

against is: "I don't know about you guys." But I don't think I've ever talked to an IT person who didn't say: "Oh yes, we can fix that, not a problem."

You find out later, it was in fact a problem. You need procedures to make sure the people that are involved in security disclosure decisions have access to the information - and get the information at a relatively early enough point to be able make the decision.

There was some language in the SEC's release that raised some eyebrows among some. It talked about the disclosure controls and procedures should not be limited to require disclosure - but to make sure all information potentially subject to being required disclosure is in the hands of those who make disclosure decisions.

I didn't view that as a scary statement. It stands to reason that you don't want the person who first notices the breach making the materiality decision. You want that information to get bubbled up into the organization to the people who do. So any disclosure controls and procedures are going to bubble up information that is potentially subject to require disclosure.

The people who make those decisions are paid big bucks to do that. So I think the controls needed in the cyber space need to ensure that there are escalation procedures so the information is given to the folks in the organization that will make securities disclosure decisions.

Lynn: Here's one issue that we all grapple with - and this is not specifically a cyber security issue but is accentuated by some of the ways in which these situations arise. The issue is that the people who are on the front lines may only see the tip of the iceberg initially on these topics - and as we've seen played out again and again, the scoping issue is tough to deal with.

Designing the procedure in such a way that people know to go to talk to somebody even on things that may not be that significant at the outset. This is probably an important aspect of the whole design process.

Then there's the human nature element of all this. If I'm someone in the IT group that is responsible for the various systems and they have been breached by someone and I noticed that, my initial reaction is to try to stop the bleeding and see if I can fix it before I go running upstairs to tell someone in the disclosure shop that we have a problem.

That's the one I find much harder to deal with from a controls and procedures standpoint, because the human nature element in these situations is to try to fight rather than flight.

Higgins: Generally, they're optimistic about being able to address the problem.

Lynn: Exactly.

Cross: There's also the issue at the early stages that you're likely dealing with some bad guys. You're likely working with law enforcement to try to catch bad guys. Disclosing the incident at that point can be counterproductive to the greater good.

That's a difficult issue as it relates to securities disclosure obligations, because there's not a ‘greater good' exception in that sense. There is a tension that happens there - and the SEC's release acknowledges that, but essentially it says you don't get a pass. Is that how you all read it?

Higgins: Yes, absolutely. I understand it that way. Dave, you want to move to insider trading?

Insider Trading & Reg FD Considerations

Lynn: Yes, if we can bring it home with insider trading.

Higgins: In the SEC's guidance, there's a brief 2-3 paragraphs devoted to insider trading to remind people that material cyber security incidents can be material information. The trading on which one is nonpublic would be a violation of securities laws.

I don't think we learned anything new about insider trading in the release that we didn't already know. It was clear that they were pushing the notion that there are other applicable insider trading rules, such as codes of ethics and insider trading policies, that companies have to promote compliance with laws that need to be followed.

They focused on them and they don't have the ability to say you must have them. They mentioned that many company policies have prophylactic policies that prevent whenever an incident occurs while it's being investigated - it causes everybody to be blacked out. A similar issue for any material event subject to a blackout is that you are forced to end up trying to prove the negative that you didn't know anything.

I think cyber incidents need to be treated probably just like any other. If you have an M&A transaction, the M&A team gets instructions that they are blacked out. This is material information and you can't trade right now. Same thing should apply in the early stages of a cyber security investigation.

I guess coincidentally the SEC punctuated this guidance with an enforcement proceeding that it brought today against someone with the Equifax breach. It wasn't one of the officers whose trading was reviewed by the special committee, but it was someone else further down the line who is alleged to have traded while in possession of information about the breach.

I think you can be sure that the SEC is going to be serious about insider trading and cyber security.

Lynn: The one issue that comes up in practice with this particular topic is that you have the scoping issue that I mentioned before. When do you close the trading window? You might have situations where the information isn't definitive enough to make a judgment as to the materiality of it after conducting a traditional magnitude & probability test.

The scary part of this is that you do have a policy in place - and you are trying to implement things like blackout procedures. How soon do you shut the window down can be a perilous decision.

Higgins: We deal with that all the time, Dave. I mean that's what we do.

Lynn: I think it's different here compared to the acquisition context or something like that. It's a little clearer for deals when it comes to the materiality from the outset as opposed to the creeping materiality problem.

Higgins: How many times have you gotten half way through the quarter, they come up and say, "Well, we're trending towards, where it doesn't look like we're trending towards the right guidance that we gave although we're still good at it. Should we open the window? Should we shut the window?" It happens in many contexts.

Lynn: Absolutely, yes.

Higgins: I think the same thing with FD. It was good that the Commission added yet another thing to remember, but in case you have forgotten there is Reg. FD. You can't make selective disclosure to certain classes of individuals and that would include information about material undisclosed cyber security incidents.

Keep FD in mind, and I would not advise anybody to change your FD policy to address specifically cyber security incidents.

Although I would go back to insider trading in your list of possible events that could be material - often you see that on the first page of the policy - throwing in a cyber incident probably wouldn't be a bad idea.

Lynn: Yes, I think that makes sense. The way they used it in the release and the insider trading and FD concepts, as well to encourage again the more current disclosure of these types of incidents.

They basically said, "If you're following S-K and get the information out there, then maybe you're not going to run into these problems, because the information is already out there."

Higgins: Yes.

Cross: It's a complicated area that companies and their counsel struggle with - what are the right answers? I think they're trying to put their thumb on the scale to favor earlier disclosure.

Higgins: Absolutely. They are trying to do whatever they can to favor it. I understand that.

Lynn: Yes. Obviously, the interesting thing about these situations particularly for dealing with a consumer-facing company that has a breach-related customer information, there's often disclosure obligations that arise completely outside of the securities context in terms of providing notice to the clients or customers and complying with state, FTC and other types of regulations that require notice.

You have this dizzying array of potential disclosure obligations - and that's really a balancing act at the outset to try to make sure you're making the right type of disclosure within the timeframe that is expected.

Cross: Then what happens when information starts to get out because you're making the required notification to customers. It complicates matters? It's one of the harder topics that we all advise on. I certainly don't think people would argue with that.

Higgins: No, I agree.

Lynn: Well, thank you very much Meredith and Keith. Also, thank you all for joining us today.