"Cybersecurity: Working the Calm Before the Storm"

Tuesday, September 16, 2014

Audio Archive

Cybersecurity incidents are happening more frequently - and are becoming more serious. And accountability for them is running all the way to the top. So the time to prepare is before they happen. This program will tackle senior management's & the board's role, as well as disclosure and liability issues. And much more. Also see next week's related webcast.

Join these experts:

- **Paul Ferrillo**, Partner, Weil, Gotshal & Manges LLP
- **Dave Lynn**, Editor, TheCorporateCounsel.net and Partner, Morrison & Foerster LLP
- **Harriet Pearson**, Partner, Hogan Lovells LLP

Broc Romanek, *Editor, TheCorporateCounsel.net*: Welcome to today's program, "Cybersecurity: Working the Calm Before the Storm." Let me go ahead and introduce our panelists. I want to thank them - they're all so busy, since this is such a hot topic. We have Paul Ferrillo, a Partner in Weil Gotshal in New York; Dave Lynn, my colleague on this site as well as a Partner in Morrison & Foerster; and Harriet Pearson, who is a Partner in Hogan Lovells and who used to be IBM's Chief Privacy Officer. She's been dubbed the first lady of privacy - she has been in this area for 20 years, which is quite a long time.

We're kicking off with Paul talking about risk management processes. What should senior management be thinking about, and to what extent should the NIST framework be considered?

Recommended Risk Management Practices

Paul Ferrillo, *Partner, Weil, Gotshal & Manges LLP*: Good afternoon, everybody. What should risk management practices be and what should senior management be thinking about? The answer to that is - a lot. This is an area that has transformed rapidly since November and December of last year with the big Target hack. It has moved pretty rapidly over the last several months, and in particular the last two weeks of August.

We could talk all day about risk management practices that should be in place at companies. I want to talk about one in particular which I think is critical - the reporting structure. How should information be reported internally, and how should information be reported up to the board? At the end of the day, it's the board which has the fiduciary duty to oversee enterprise risk management and cybersecurity.

Where we feel there is a lack sometimes is plain English communications from management - the CIO and the CISO and others - in terms of reporting incidents, responses, impacts and events to the board in a way that's both timely and effective, and which conveys the information necessary for the board to be able to understand what's going on.

As part of any risk management process, you obviously need a very healthy, robust, war-gamed incident response, disaster recovery and disaster planning response plan in effect and ready to go at any particular time. But I think the information unfortunately gets lost when it goes from management to the board.

Boards tend to have a lot on their minds and are focused on many different things. The whole concept of quality and timely information getting to the board is critical, because, again, it's the board that has to help and guide the company in allocating resources properly to various areas related to cybersecurity.

This is an area unlike others in corporate governance, where we are often dealing with a robust governance structure. In particular since 2002, after both Sarbanes Oxley and FASB and other financial reporting standards, boards are rather well equipped to have discussions about financial reporting and controls. But when it comes to cybersecurity, there are no "rules,"

there are no "standards," and there are no "guidelines."

We have been referring many of our clients to something called the National Institute of Standards Cybersecurity Framework, which was published by White House in February 2014. I would refer you to the document - you can find it on Google. It is somewhat complex but at the same time is somewhat easy to understand.

NIST is a set of cornerstones of cybersecurity which companies should be focused on and a set of profiles and implementation tiers. It is designed to help companies understand where their cybersecurity procedures are today, at this point in time, and then help them set goals to understand where they hope their cybersecurity practices will be if they improve and do better in certain areas.

The most interesting thing about NIST, from both governance and litigation perspectives, is that it is, for lack of a better term, a standard. It is something that is documentable. It is something you can have discussions about between boards and senior management on issues related to cybersecurity. In fact, if documented correctly, we feel it could help put companies in a much better position if they are later breached and then become subject, like Home Depot and Super Value, to litigation which alleges that the companies did not conform to cybersecurity "best practices" - whatever the heck that means.

NIST is at least a procedural framework to allow companies to have the types of risk management discussions around cybersecurity in a common language and in a common format to allow some dumb lawyer like me to say in court, "We did the best we possibly could. Here are documents, board minutes and evidence showing what we did."

So, Broc, that's a great question about risk management. I think it all starts with reportable information and documented evidence of what a company is doing with respect to its cybersecurity procedures.

Romanek: Does anyone have anything to add about the Framework?

Harriet Pearson, *Partner, Hogan Lovells LLP*: I'll make a couple of comments on the NIST Framework. Before February 2014, when the NIST Framework was issued by the White House, if you were to have asked senior management and IT security leaders at companies - What standard are you following? Where is the rule book for IT security? - they would come back at you with binders full of ISO standards, NIST papers and other things that were much more technical and process-oriented. The NIST Framework, as it was issued, reflects the work of 3,000+ individuals, developed in a very open and actually pretty decent process that was run by NIST in collaboration with the White House and multiple other agencies of the U.S. government in the past couple of years.

It is a document that is exceedingly accessible by all types of management as well as technical professionals. I agree with Paul that it is a useful document and can be the basis, at senior management and corporate-wide levels, for documenting the steps the organization has taken.

But I think organizations that choose to use it need also to have their eyes open as they do so, on two levels. One is that the Framework, in its title and its explicit approach, is designed for those companies that are in the critical infrastructure. There is not a lot of information in the Framework describing what that word means. It is a term of art that has emerged in the cybersecurity space, indicating those kinds of companies that are essential to keep operating - where failure is not an option.

So as you use the Framework, consider whether your organization is that kind of an organization. That doesn't mean that companies that are not in the critical infrastructure shouldn't use the NIST Framework. But just understand that it's written for that kind of organization to begin with.

The second consideration before you might adopt the Framework is that it does create a road map. If an outsider, a plaintiff or anybody else wanted to see if you were following the road map, they can say, "I know from the Framework that you should have done the following. Please give me the document associated with the training or the policy or the incident response, etc."

The use of the Framework creates a common language that everyone can speak, which is a very good thing if you're trying to progress the security posture of a company. It's a very good thing if you're trying to simply document what steps you've taken. But there's a downside in that transparency of a common language. It also makes it easier for third parties to ask about what you did and didn't do.

I agree that it is now becoming more and more a *de facto* standard in the private sector. There is precious little else out there that is at this level of generality and that is accessible to all levels of the company. And that is exactly what it was intended to be when it was put together as a strategic project coming out of the current administration.

The Board's Role and Board Committees

Romanek: Thanks. Let's go ahead and move onto our next topic - the board's role, and which committees are responsible for this area. Harriet?

Pearson: When you're talking about using the Framework, one very important constituency here is obviously the board and its role in oversight.

Fundamentally, effective oversight of cybersecurity does not mean that anybody on the board is going to have to become an IT security specialist or technology expert. But it really does behoove anybody serving on the board these days to get familiar with the questions that they need to be asking.

There are several sources of where the questions might come from. The NIST Framework is indeed actually one place to get a set of questions. I'll boil it down to a just a few points. I have a longer checklist that I use personally when we do this kind of work.

The first question that the board should ask is, has management identified the known cybersecurity risks to the company? Has the company done an assessment?

Going back to risk management processes, first you have to assess what your risk profile looks like. Are you in the financial industry, the retail industry, or the health industry? Who is about to come and attack you, and what are they looking to get? Are they looking to get payment data? Are they coming to disrupt operations, to make a political statement or to do something else?

Understanding the threats to the organization and then understanding where your most valuable mission-critical data or systems are is the first step. For the board, asking management to describe what they've done in that sense is the first question the board should definitely be asking. Then the board should ask about any audits or vulnerabilities that the company has had, or whether there has been an incident.

A second question in terms of board oversight would be to ask what management has done to develop appropriate safeguards to protect their systems and the data in a risk-calculated way.

If I'm in management, I would like to describe what I've done using some sort of industry standard or benchmark that I can point to, so I could say whether we were on par with or ahead of where industry standard might be. Listening to management describe whether the program that they've put in place aligns with the industry standard is a good test if you're a board member.

Is there appropriate leadership of that program? Can you meet individuals leading it and assess the quality of their work or the quality of their leadership? Is the workforce trained on these issues? Those kinds of things are important in terms of assessing management safeguards.

Is management aware of or have they implemented methods to detect if something happens? We've been reading about a lot of incidents and breaches. What has the company done to detect them and to report them internally, so they can be assessed for their severity?

Are management and the company ready to address an event? A company which has a program ready to go and has practiced it is going to be able to handle an incident better than a company for whom it's the first time it's actually getting its folks together and trying to figure out which forensics firm to call, which law firm to call, or which government agency might be helpful to them. There are huge differences between companies.

As a board member, asking about readiness is a part of the essential list of questions to ask. If something were to happen and operations were to be disrupted, are you ready to come back up, with business continuity disaster recovery planning? Those are the kinds of questions that we see, and that we counsel board members to ask.

In terms of which board committee is responsible for this area, it depends on the company. The full board should at some point - probably annually is a baseline frequency - be briefed and be made aware of the profile of the organization and the steps the organization is taking to manage cybersecurity risk.

From a committee perspective, the majority of organizations are looking at their audit/compliance type of committee as the committee that gets deeper. The trend being reported in some of the trade press is that some members of audit committees are now being selected based on their technical or security type of background. I think it's becoming true particularly for companies that are in some of the higher-profile, higher-risk sectors, such as the financial services industry.

That's my sense of this. I don't know if any of the other panelists might have a view as well.

Ferrillo: With respect to board committees, Harriet, I think that ultimately there's not a one-size-fits-all solution. Post-financial crisis, a lot of enterprise risk management functions were given to the audit committee. In fact, many audit committees still lead not only the audit function but also the risk function.

The problem, obviously, is one of time. I was participating in a panel recently where the panelists were talking about boards being informed of what was going on in cybersecurity. I heard that the average time spent by the full board on this topic was seven minutes a year, which I found both interesting and shocking at the same time.

However boards want to structure their committees, and whether they want to create a standalone cybercommittee, is certainly up to them. The point that I hear over and over again, though, is that it's not just the committee structure that matters.

It's the information that's getting to the committees, to help these board members make appropriate decisions within their fiduciary duties as directors.

Cybersecurity Training

Dave Lynn, *Partner, Morrison & Foerster LLP*: How about the concept of sharing the information organization-wide? What sort of training is happening or should be happening for everyone in the organization?

Pearson: The training question is deceptively simple, because it goes to what is the objective of the training. For the most part, the objective of training the workforce and maybe the extended workforce, *i.e.,* contractors involved in carrying out your company's operations and mission, is to help them be sensitive so that they don't do something careless – that that they don't, for example inadvertently click on an infected link or fall for social engineering scam. Physically, it means they won't open the door and let somebody in who then compromises a particularly sensitive IT system.

So the training is meant generally to arm the workforce to a baseline, "Let's be smart about things." That kind of training is simple to do, and it needs to be simple, in order to be observed by everybody. But it's actually hugely hard to deliver that kind of training effectively.

Some companies want to say they have trained the workforce, so they can check the box that they have done compliance training. But there is a huge difference between checking the box and actually completing training effectively, in order to permeate an organization's culture and change people's behavior enough so they actually are more careful.

I've been on the inside of companies in the energy industry and at industrial companies where safety is very much part of the culture. Before a meeting starts, you have a safety briefing. Everyone is very tuned in and conscious of safety issues. I believe, based on historical trends here in terms of cybersecurity risk, at some point almost every kind of company will have to have some sort of culture around safety in terms of protecting systems and data. While we all cannot become experts in computer security - that's not reasonable - all of us can become experts in how to be thoughtful about interacting, particularly those who have access to sensitive data.

The NIST Framework has a section on workforce training. I think it has actually has four types of training. If you're going to follow an industry standard, it's useful to be aware of those four types, so you're not running afoul of compliance with the standard.

So there is training for all workforce in the NIST. And there's a special reminder that so-called "privileged" users, *i.e.,* those employees who have higher access to systems based on their roles or who have some special information, are actually a very high risk element to the population.

Make sure that third party stakeholders, your key vendors, for example, or partners who might have access to systems or information, are aware of their obligations and their security issues that are relevant for them, for your risk profile.

Finally, for the type of audience that is with us today - senior executives and the board - make sure that they are familiar enough and aware enough of their particular vulnerabilities and the actions that they might take as individuals as well as overseers of the organizational function.

Those are couple of thoughts about training - the fact that there is a variegated population that can be addressed by training of certain types, and the fact that it is actually a vital element. It's not a particularly technical thing to do, but it's a vital element of a cybersecurity plan.

And the information being conveyed, particularly when you're dealing with senior executives, needs to be thought through in terms of content so you're not saying something you'll regret later, but you're saying enough to get them to be mindful.

Does anyone have any other thoughts?

Lynn: Another area that has been important in some of the breaches that we've seen is to be ready to train employees when a breach actually happens, how they should be responding the clients or customers, and what they should be doing to maintain customer relationships and to communicate whatever needs to be communicated in a way that's consistent with the company's overall plan.

Having a plan like that on the shelf ready to go is probably not a bad idea, particularly for some of the most sensitive areas like retailing and the like.

Ferrillo: The problem, though, with having that sort of plan on the shelf is that it could get dusty sometimes. I think that the organizations we are seeing today understand that this game is not about firewalls. It's about detection response and recovery.

Incident response plan and event response plans need to be practiced. They need to be war-gamed, and they need to involve all of the critical employees and layers of your organization.

We know one Fortune 50 company that war-games their incident response plan up to the CEO level, to make sure that senior management is involved as well. So planning is great as long as it's practiced.

The PR/IR area of cybersecurity is particularly interesting. I would say that it's particularly counterintuitive to those who have done other sorts of crisis management and crisis planning about how they communicate. Many times, in the cyber area, you're not allowed to communicate because there's an open investigations by Treasury, Secret Service, Justice and the like who don't want you to say anything.

Dave, as you've said, you have a dichotomy now of companies that are communicating, but have gotten hammered for not communicating enough, versus those companies who have not communicated all that much, but have escaped or gotten under the radar screen, maybe because the American public is numb right now to the number of cyberbreaches and cyberattacks. We could spend all day talking about disclosure and PR/IR. But it's certainly something where, again, it's great to have a plan, but it needs to be practiced and well thought out.

Pearson: I think having senior management or executives doing war games or table-top exercises is a great point. Traditional compliance education, where you look at a screen, watch a scenario, then click on an answer, is good. But nothing beats actually going through the motions of, "Something has happened, what do we do? If something is offered to you, what would you respond?" I have been part of table-top exercises, including at the CEO level. You can absolutely tell that the capability level of all of those involved goes up, and that personally, they become much more aware.

And, while I have not personally done this, I have heard of at least one or two companies that have done this at the board level. That's a very powerful statement and that indicates an investment of time that goes well beyond the seven-minute average, if that's indeed the case.

For certain organizations, that may actually be a little edgy but advisable way to handle something like this. It really makes a statement.

D&O Insurance

Lynn: In terms of our focus on what the board should do and how they should be involved, one question - and this would apply equally to the executive officers - is to what extent does insurance cover things that may happen in connection with these types of situations, and to what extent does it not cover situations? I'll turn it over to Paul for that one.

Ferrillo: Dave, that's a terrific question. You're getting into areas of great misconception in the business community, about how to provide some sort of insurance coverage for cyber-related attacks.

On the directors and officers liability insurance front, the coverage is limited in many respects to board coverage for breaches of the fiduciary duty of care, for failure to oversee the cybersecurity procedures of a company. We would call that in the business a *Caremark*-type claim. It could be filed in some state court, Delaware Chancery court for instance. That would be covered.

There have been very limited amounts of cybersecurity securities class actions that have been filed after the announcement of a breach if one were to happen, as was the case with Target. That would be another type of claim that would be covered under a D&O insurance policy.

But what many companies now have come to understand - again, really driven from a risk management enterprise risk management function - is the availability of cyber insurance to cover cybersecurity related breaches. Just as when you're driving a car, it's best to have auto insurance, with respect to a cyber-breach, you can now have direct insurance that covers the direct first party and third party effects of a cybersecurity breach.

There are a number of tremendous advantages to companies having cybersecurity insurance. Many Fortune 50 companies might not need them, because they have the infrastructure setup in their general counsel's office to do the types of things they need to do. But for smaller companies, cyber-insurance can provide coverage, such as coverage for the costs of customer notification based upon state law, credit checks and monitoring, business interruption insurance, cyber-extortion coverage, forensic costs and lawsuits brought by third parties such as banks against credit card processing facilities like Heartland Payment Systems.

Cyberinsurance is the new mantra for cybersecurity risk management. It's something that I would urge all companies to consider thoughtfully. The fact is, there are only two types of companies out there - those who have been hacked and those will be hacked again.

Documenting Preparedness

Lynn: The next point we should cover is how you document or memorialize everything that you've done for you preparedness here, so that in the event you're facing a lawsuit or for other purposes, people can look back to what the company has done to get itself ready for these types of situations.

Pearson: This is a really important question because it goes to the heart of prevention and risk management in this area. The IT department, security professionals and others have a big job to do with managing the technologies and the processes necessary to protect the company.

The in-house counsel, general counsel and similar advisers also have something to do to protect the company. First, there are fair number of legal issues implicated by actions taken to secured networks and secure organizations. If you ramp up monitoring of systems you end up running head long into privacy laws, possibly in the United States, and particularly internationally. If you're engaged in information sharing and collaboration with law enforcement, those are thorny issues to address and to manage. So there are legal issues and a role for in-house counsel in the actual cybersecurity risk management effort from a technology standpoint, and in supporting the process work of a company.

At the end of the day, the core issue here, if you're advising an organization before an incident happens, is to design your activities to enhance the company's cybersecurity posture. You don't want to create damage if something were to happen. You want people to be able to look at the communications, the documents, the e-mails and everything else that has gone into making the company's cybersecurity better.

Part of making things better is to acknowledge your current state. The NIST Framework, as an example, prompts you to actually document your current state and the gap between your current state and your desired state. Some of the words in the NIST Framework actually invite you to declare that you might be marginal, and that, because of the nature of the organization that you are in or the risk profile of your organization, you might not be aspiring to a very high level of cybersecurity. All of those kinds of word choices and the posture that you might document, or the carelessness with which employees or others might be communicating about incidents, can leave the kind of document trail that could have words in the record that might be injurious later on.

As I've been working with organizations about this area, the practical counsel I've been giving focuses on a couple of different things.

One is, if you're having interactions with the board of directors around cybersecurity, that's a wonderful time to prepare authoritative recurring sets of documents that describe the organization's cybersecurity posture, the program and the corrective or the improvement actions that are under way.

Every single organization has an improvement action or corrective actions under way. It is no big secret, at least not anymore, that those things are happening. But having a carefully vetted document that is authoritative and that represents the full range of disciplines and thought processes of an organization is vital to counter perhaps other less fully informed e-mails or documents that might be in the company's coffers.

So that's one thing and well worth the exercise. You're going to have to do it anyway to keep your management and your board properly informed.

The second thing goes back to employee awareness. The IT and security professionals who are involved in executing the organization's cyberplan and program need to be introduced to and educated about the appropriate ways to carry out their mission. Most of these folks are highly trained, highly capable professionals, who are very used to dealing with sensitive topics. But every now and then, and I think particularly in the height of an incident, you might see some language that you might later regret.

I think there's also a specialized kind of training and sensitivity to issues and language which that population might very well benefit from. Increasingly we do a lot of privilege training, not just for in-house counsel but also for broader communities of security professionals, to introduce them to appropriate interactions with lawyers and how to think about language well beyond when it's time to try to assert and use the privilege to have deliberate conversations about legal advice. We also, just generally, cover sensitivity about language.

Those are couple of thoughts about memorializing preparedness, and avoiding the counter of that, which is the memorialization of either speculation or other kinds of information, which is not particularly useful because it just doesn't depict the organization as it is.

Lynn: Are there any other comments on that topic?

Ferrillo: No.

Disclosures About Cybersecurity Preparation

Lynn: The last thing we'll talk about is the disclosure that comes either before or after a cyber-attack. This is a topic, as most people are aware, that the SEC has been fairly focused on over the last three years or so. As is often the case, a lot of that focus is generated by continuing interest in the Administration and in Congress, trying to advance a cybersecurity agenda and focus people's attention on potential risks that are out there.

As we've seen time and time again, sometimes Congress and other policy-makers see public disclosure as a way of focusing

people's attention on an issue. Some of the inquiries that were made of the SEC by folks on the Hill ultimately prompted, back in October 2011, the SEC Staff to issue guidance in the form of a CorpFin Disclosure Guidance Topic, which has been the basis since that time for how we approach the disclosure issues around cybersecurity.

Even though that guidance happened about three years ago, this issue is by no means falling off the radar at the SEC, or among investors and the public either. We continue to see things happening at the SEC. There was a Round Table on this topic, and there have been continuing inquiries from Congress. In some cases, members of Congress have asked that the SEC upgrade the guidance or to take other steps to try to improve the disclosure with respect to this topic.

Since the guidance came out in October 2011, we've seen the SEC Staff expressing its views in their periodic reviews of company filings, issuing comments, seeking revised disclosure, perhaps in future filings, to more specifically address some of these concerns.

I was going to walk through some of the things that the guidance originally said and what we've learned since that time from the Staff. I think probably the best summations about what the Staff expects comes from a speech given by Shelley Parratt, who's the Deputy Director of CorpFin, in May 2014. She outlined some of the things that companies should think about in writing disclosures around cybersecurity. How should the information submitted to the Commission be updated with respect to threats and as risks changed over time? How would the company respond in the event of a material breach? Are there aspects of the operations that particularly give rise to material cybersecurity risks? And what are the potential consequences and costs that might be associated with any particular cyber incident?

I think probably the most important disclosure, from the Staff's perspective, is whether the company has experienced some material cybersecurity incident, and if so, whether the disclosure about that incident is current.

In CF Disclosure Guidance Topic No. 2, the Staff acknowledges that there is no direct line item that they can point to that says a company must disclose cybersecurity risks. Rather, the guidance says that, on an ongoing basis, the company needs to evaluate its risks against existing disclosure requirements.

The list that they put in the guidance was list that we're all familiar with all, and which also appeared in Staff guidance on climate change disclosure: risk factor disclosure, the MD&A (Management Discussion and Analysis of Results of Operations and Financial Condition), the description of business, the description of legal proceedings and even the financial statements, to some extent, are all affected. I would probably augment that list today by saying, closely related to risk factors, you should definitely, on an ongoing basis, look at the forward-looking statement disclaimer, and whether the types of risks and uncertainties that are identified there adequately address cyber-risk.

Also, in the proxy statement, look at the disclosure about the board's oversight of risks. I think increasingly that will be the area where people will be looking to see if there is anything referenced about the board's oversight of particular cybersecurity risks - maybe not across the board, but certainly in those industries where the companies may be particularly affected.

Best as we can tell from some of the correspondence that has gone back and forth from the SEC Staff to the Hill, after the guidance came out in October 2011, there was a concerted effort to look at the disclosures about cybersecurity in the next batch of Form 10-Ks. I think it's becoming ingrained as more of ongoing effort to look at this disclosure as the Staff goes forward in time.

A lot of comments from the Staff echo many of the themes from the October 2011 guidance. The Staff is concerned about situations where the company talks about cybersecurity too generally, or lists risks that would apply to any company, without getting into specific risks that could potentially affect their particular company.

Another important area, when you look at the Staff comment, is if in fact cybersecurity has affected the company or there has been a breach. In most cases, the Staff is looking for information about a material breach. But I've even seen comments where the Staff has asked if there has been any breach. The Staff doesn't consider the risk disclosure a purely theoretical exercise. They want to know what the company has experienced in this area and could potentially experience in the future.

Often what the Staff is looking for is more details in terms of potential consequences and costs. When a company is not dealing with an active breach or a recent breach, and even what it is dealing with that situation, it is difficult sometimes to respond with specifics around consequences and costs until more information has been developed. So I think there has been some reluctance on the part of issuers to put that level of detail in the disclosure.

Another area where I've noticed Staff comments is when a company has cybersecurity lumped together with other potential catastrophic events. I've seen comments where the Staff basically says that if cybersecurity really is a potential risk you should have it as a separate risk factor, with all of the details I was just describing. The Staff will often ask whether there have fact have been breaches, or if there's a possibility of a breach going forward, and what are the potential risks for the company and the consequences overall.

What do you disclose when you have actually had a breach? In some of the comments since the guidance was issued, the Staff is concerned about what the company is saying, particularly in the MD&A and notes to the financial statements, about resulting consequences of a breach that has occurred.

One of the challenges in a situation when you have an active investigation of a breach is what you can say at what point in time. How much information can you get to the marketplace? As was noted earlier, it is often very much a consideration, when you have an active investigation, that law enforcement may significantly limit your ability to speak about certain aspects of the breach. That has to be factored into the disclosure approach.

Companies often try to write disclosure about a cybersecurity breach by analogy to other types of crisis situations. But as noted earlier, a cybersecurity breach may not be easily comparable in all cases.

In terms of the disclosure, when you have, for example, a material error that's identified in the financial statements, and you're about to commence an internal investigation and potential restatement, a lot of times the company is very circumspect about the information they get out to the marketplace, both at the time of the initial announcement and then thereafter in subsequent earnings releases or periodic reports, simply because you don't know what you don't know, particularly at the beginning of the event.

I think that's something that you run into with these types of investigations of actual breaches at the outset of the inquiry. It's very difficult sometimes to have an idea of what the scope and significance and ultimately materiality of this event will be, because you just have not gathered enough information to know how much was affected and what the consequences of that compromised data or intellectual property or assets will be.

Looking at the Staff guidance and some of the comment letters we've seen, the Staff is trying to communicate that your disclosures should talk about the scope and magnitude of the breach, whether it was material and whether there has been any known potential cost resulting from the breach. They also want information about preventive measures that you might take in order to the reduce the likelihood of a repeated incident like that. More specifically along those lines, they want to know what sort of remediation costs are associated with a breach. That might range from things such as liability from the stolen information or assets to what sort of incentives might be offered in order to maintain customer relationships with business partners that may have been affected significantly by the breach.

The notion is, that once this has happened to you, you're going to increase protection costs, because you're going to have to make massive changes to the systems and environment of the organization to try to head this off from happening again, including things like organization changes, personnel costs and technology. All of those things, the Staff has noted, might be the types of things that you would have to address.

Disclosure should also address ultimate business aspect in terms of loss revenues that might occur, as well as things that are more amorphous like reputational damage that could have adverse consequences for the ongoing business activity. Lastly, disclosure should address the prospects for litigation and how that might play out at the company.

I think those are the types of disclosures companies need to focus on when they are in the post- breach situation. Obviously, as we've talked about, there has to be a lot of effort and coordination in terms of the messaging. A lot of the times in these situations we've seen a very active effort to communicate with customers or clients in a very public way and to be ahead of the situation as much as possible. At the same time, I think you have to look at those disclosures through the lens of potential liabilities you might have from a federal securities perspective as well.

Are there any other comments on the disclosures from the panel?

Harriet and Paul, thank you very much for joining us here today. And thanks to everyone in our audience for listening in.