Joel Reidenberg:

Good morning and welcome to the SEC Historical Society's Panel Program, Morgan Lewis Presents 2017, understanding cybersecurity regulation, perspectives from federal and state regulators. We are broadcasting live from Morgan Lewis LLP office in New York City and online at www.SECHistorical.org.

My name is Joel Reidenberg; I am the Stanley D. and Nikki Waxberg chair and professor of law at Fordham University where I founded the Center on Law and Information policy. I will be moderating today's program.

Since its debut in 2009, this series has examined cutting edge issues in financial regulation of interest to the legal profession. The series is made possible through a partnership between Morgan Lewis and the SEC Historical Society. With more than 2,200 legal professionals in 30 offices in North America, Europe, Asia and the Middle East, Morgan Lewis provides comprehensive litigation, corporate e-finance restructuring, employment and benefits, and intellectual property services in all major industries. The SEC Historical Society through its Virtual Museum and Archive at www.SECHistorical.org shares preserves and advances knowledge of the history of financial regulation.

The Virtual Museum and Archive is the preeminent online source for original and primary material on the regulation of the capital markets. Previous programs in this series are permanently preserved in the Virtual Museum and Archive on the website under programs in the dedicated Morgan Lewis Presents section. Past broadcasts have examined such topics as current issues in broker-dealer enforcement, asset management, criminal enforcement of securities laws, harmonization of the regulation of investment advisors and broker-dealers, and the enforcement after the Dodd-Frank Act.

All of these programs are accessible in the museum free of charge. I would encourage you to check them out at the end of this broadcast.

The SEC Historical Society is grateful for the generous sponsorship of Morgan Lewis for today's program which will examine the history and evolution of cybersecurity through the lens of federal and state regulators.

Before we get started I should mention that all in-person attendees requesting CLE should sign in at the registration table, and those folks on the phone should listen for the code announced later during the program.

Joining me on the panel this morning, I will introduce our speakers in the order they are seated next to me. First, Susan Axelrod: Susan is the Executive vice president of Regulatory Operations at FINRA. In this capacity Susan oversees enforcement, the office of

fraud detection and market intelligence and member regulation. Before being named to her current role she was executive vice president and head of member regulation and sales practice with responsibility for ongoing surveillance and examinations both routine and investigative of FINRA securities firms.

To her left is Mike Pieciak, Mike is commission of the Vermont Department of Financial Regulation. He was appointed by Govern Peter Shumlin in July 2016 and reappointed by Govern Scott of December of 2016. Michael serves as the chief regulator of Vermont's financial service sector including the insurance, captive insurance, banking and securities industries. He previously served as the deputy commissioner of the department's securities division.

To Mike's left is Tim Burke, Tim is a partner here at Morgan Lewis and head of the securities enforcement and litigation practice. Tim handles a wide variety of both securities regulation as well as litigation matters. He represents broker-dealers, investment advisors, registered representatives, senior management, compliance officials and others in connection with private and public investigations and enforcement proceedings brought by the SEC, FINRA and other regulatory organizations, as well as numerous state regulators.

And to his left is Meredith Cross, Meredith is a partner is the transactional and securities departments and a member of the corporate practice and strategic response group at Wilmer Cutler Pickering Hale and Dorr. Meredith advises public companies and their boards on disclosure and other corporate finance securities law and corporate governance matters, including SEC enforcement matters involving corporate finance. She has served as the director of the division of Corporate Finance of the SEC.

With that let us get started. We have had the pleasure of working together planning this program so we will jump right in.

Let's start with a brief discussion of the history and impetus of regulatory interest in this space. I'm going to ask Meredith to start us off, and talk a little bit about when the federal regulatory interest began for cybersecurity.

Meredith Cross:

Good morning everyone, from the SEC's perspective, the interest in cyber started in earnest when I was there. I was there from 2009 to 2013, and in that time period is when things like denial of service attacks became prevalent, malware running through company systems became prevalent, and credit cards getting hacked through retailers. All those things started to get a lot of attention and so a lot of people were looking at a way to deal with this. Policy makers wanted to find a way to deal with this, and similar in many

respects to when Y2K, year 2000, was happening. I left the SEC the first time shortly before year 2000. A lot of people thought that if you required companies to disclose what they had for cybersecurity and if they didn't have anything that would be very embarrassing so they would have to come up with something so they could then say "here's what I have for cybersecurity." So a lot of people were looking to the SEC for pushing on disclosure to cause companies to shore up their defenses.

While that was going on, at the same time Senator Rockefeller was very interested in hearing about the SEC's disclosure efforts, including about cyber breaches. He sent a letter to Chairman Shapiro in May 2011, and she wrote back shortly thereafter describing the disclosure requirements; he was introducing legislation to require disclosure. After that the division of corporation finance put out the guidance that is the current existing guidance about cybersecurity disclosure. We issued it in October 2011. So that sort of started it off, that's on the public company side.

The regulation of regulated entities and what they needed to have was on a different path, and I think others on the panel can talk about that.

Joel Reidenberg:

Mike do you want to talk a little bit about the state level?

Mike Pieciak:

Yes sure, I'd be happy to. Good morning everybody; it's great to be here with you all today. I think at the state level there was also response from the 2011, 2012, 2013 time period from major breaches that had occurred. Major companies and the states look most specifically at the regulated entity side. From the state regime, the investment advisors under a hundred million dollars asset under management are exclusively the jurisdiction of the states, and that is the category that we saw as having potentially the most exposure because they may also be the entities that have the least sophisticated regimes in terms of protecting, defending and mitigating cybersecurity issues.

So in 2014 NASAA, the North American Securities Administrators Association, conducted a survey of our investment advisors and found a couple of things that were somewhat concerning. There was a very high percentage of them that didn't have any policies in place on cyber, and a very high percentage that didn't have cyber insurance. In 2014 that was still sort of an evolving insurance product, but I think it was over 60% of those advisors did not have cyber insurance of any kind.

The number of individual states responded, including Vermont, by requiring our investment advisors to have specific plans in place; have annual risk assessments; to have

cyber insurance as well. It's a mandate in Vermont for the appropriate size IA depending on what the business model is of the IA and how big their company is.

In any event, we released a survey this week actually that serves as a follow up to this original 2014 survey, and some good news was that the 2017 report that we just put out shows a highly increasing number of IA's have cyber insurance. I think out of 1,200 examinations that we conducted on a coordinated basis through the early part of 2017, only about 44 of those companies did not have cyber insurance. So that was a good sign. A very small percentage did not have any cyber policies or risk assessment in place, which was another good sign.

In any event, the states have been taking an active role and the industry itself has been responding as well.

Joel Reidenberg:

Susan you wanted to add something?

Susan Axelrod:

I was just going to make a point with respect to FINRA and the importance of cybersecurity. We went back and looked at our priority letters which we issue every year and going back to about 2009, with one exception, this issue was in the letter to continue to highlight for firms; focus on this; this is a key risk for the industry.

Even going back to 2006 and 2007 letters covered topics such as business continuity planning and protection of customer information.

It's interesting one of my colleagues today is sitting in a conference across the globe with international regulators; this is one of the key issues being discussed at the conference. So regardless of the history I think this is an area we're all going to continue to focus on regardless of our specific jurisdiction responsibility for years to come.

Joel Reidenberg:

Meredith, if I could come back and ask you something that was sparked by Mike's comment; at the federal level was the SEC also concerned early on about lack of cyber risk insurance for companies? I thought it was really interesting that an important focus on the state level was to be sure that the advisors had insurance coverage. I don't recall hearing that coming from the SEC and I just wondered if it was a function of the timing since you were looking at the issues a couple years later. But Meredith I wondered if you could comment?

Meredith Cross:

And I'm talking about public companies as opposed to regulated entities, but in the disclosure guidance, disclosure guidance Topic 2, was a new guidance that we started doing when I was the director. This one in particular mentions that when you're talking about risks posed by cyber, one of the topics to talk about is through the description of your relevant insurance coverage.

The SEC doesn't tell public companies to have insurance, it doesn't tell them to do anything other than report and have internal controls and those sorts of things. But they do want investors to have appreciation for what kind of exposures companies have and if absence of insurance would be a material risk for a company, then they would need to talk about that, and that is in the guidance.

Mike Pieciak:

Just to jump in on the cyber insurance marketplace, I think it's still a highly evolving marketplace. The coverages are not ubiquitous yet in terms of what the exclusions should be, what the language should be, what the lexicon is, so there's a lot of work to be done even in the insurance space in terms of what are the appropriate coverages, what's the appropriate amount, and what are the appropriate exclusions. And it's still important even though people have cyber insurance to determine what the exclusions are, because they can actually be pretty light policies depending on what's in them, but that's something that's continuing to evolve over time and I think we'll see more and more public and smaller companies acquire cyber insurance.

Susan Axelrod:

I was going to say for smaller companies that have less resources you don't want the fact that someone may have cyber insurance to say "okay now we don't have to invest in the real protections and infrastructure we need," so there's got to be a balance in terms of how those resources are spent and companies have to continually be thinking about where there are vulnerabilities and how are we going to fix them. You don't want a false sense of comfort to say I have this insurance; you want people proactively thinking about, reading about, understanding all that's happening in the environment so they're making sure they're addressing it and risk assessing it appropriately for their firm.

Joel Reidenberg:

After this initial wave, what were the responses from both the regulatory side and perhaps the corporate side as well to the documents issued respectively by the federal and the state regulators?

Meredith Cross:

From the SEC side I would say the companies very quickly started looking at their disclosures and enhancing their disclosures about cyber and as they did that, that I think probably led them to enhance their cyber defenses. The SEC staff issued lots of comments in the year or two after the guidance went out, and for example if you didn't disclose breaches and they could find references to breaches online then they would say "don't talk about this hypothetically," that kind of thing. So there was a pretty intense effort to enhance disclosure post-guidance, and I think there was a terrific improvement in companies' disclosures, which I think probably also coincided with enhancing what they were actually doing so they would have good things to say.

I don't know, Tim, if you have that sense from outside the government.

Tim Burke:

I think it's been an evolving sense and good morning everybody, I'm Tim Burke. Nice to be here as well.

In the regulated company space the SEC just last month published what they called Cybersecurity Initiative 2.0, and it was a report of an examination program they had started earlier in the year. The leading observation that the SEC made was that the registered companies have improved greatly in the area of having policies, procedures, testing, and validation much more so than just three years earlier when the 2014 cybersecurity testing occurred. I think people have heard the message, I think they've initiated policies and procedures and now we're at a level where are the procedures sufficient enough, and that seems to be the area where regulators are focusing today.

Meredith Cross:

Recently Chairman Clayton has said that he wants the disclosure guidance revisited, and he has said he thinks there should be additional disclosure, so I think these things do come in waves, so this is an area of focus for him. And so I wouldn't be surprised since he, and the senate banking committee recently wrote to him and asked them to revisit the guidance, and he already said he wanted to. So I wouldn't be surprised if this now gets refreshed.

Joel Reidenberg:

I guess that means we have to come up with an appropriate disclosure for the systems organizations are using. Let's turn to the topic of inspections and enforcement of regulated entities and perhaps, Tim, if you want to kick this one off, what sort of inspections and enforcement approaches were the regulators taking?

Tim Burke:

Sure, as I alluded to a moment ago the SEC just last month released the report on Cybersecurity 2.0 examination and inspection results. The SEC in the last year had examined 75 different firms including broker-dealers, fund companies, and investment advisors, and they focused mainly on six areas those were internal governance and risk assessment, access rights and controls, data loss prevention, vendor management - which is something we're going to come back to I think and talk about in more detail - Internal training, and then finally incident response.

As I said overall there was a conclusion that firms had by in large all adopted policies and procedures to address those areas, but the SEC did issue some observations in the areas that could benefit from improvement, which I think we should all take as sort of a warning shot message that if you don't meet these standards then you are subject to regulatory criticism.

The areas that the SEC said fell into the categories of issues observed included firms that had generic cookie cutter type guidance without any specific details. So if your cybersecurity policies aren't specific in terms of the business model of the firm then you're vulnerable to regulatory criticism.

Another area of concern is firms that say certain things in their policies and procedures but don't live up to them. For example, firms that say they're going to do regular testing but only do it once a year, or firms that say that they have an annual requirement but do it less than annually. Those are things that when the examiners come in and they do their testing, and we work with a lot of broker-dealers in the exam phase, or are undergoing exams. Those are areas that you want to be mindful of, you really want to go back and look at your policies and procedures and verify things like "what is the frequency required" and are you living up to your own standards.

Again mandatory training that's not in fact required training is something that firms should pay attention to, and then finally the issues observed included inadequate system maintenance such as failure to install software patches or upgrade operating systems through software installments are areas where firms have vulnerability as well.

From a regulated entity point of view, Susan, I know your folks dive into this deeply on the FINRA side, maybe you could speak to some of the things that examiners are doing in FINRA with respect to these issues?

Susan Axelrod:

Absolutely, and this is an area as I mentioned before, it's been publically a priority and it will continue to be a priority.

As regulators we have a number of tools in our toolkit in terms of how we want to deal with and address issues in the industry. I think with respect to this one in particular you want to achieve the right objective. We have not been active enforcers, so we haven't brought a lot of cases, we don't have a specific cybersecurity rule.

My view often is if you get to an enforcement case something bad has already happened. A customer may have been taken advantage of; there may be a supervisory issue or some kind of breakdown in the firm. As regulators, we can do a much better job of trying to work with the industry to prevent these things from happening, and with respect to cybersecurity there's an active role that we try and take on with respect to education, keeping firms aware and during the course of examinations making recommendations to them. Because we actually do get a look across the industry and it's not just the large firms and what they're doing because they have a lot of resources; there are a lot of small firms out there that need to focus on this as well that may not have access to the same level of information, may not be able to hire former homeland security folks to work at their firm.

The balance of being a regulator and the balance of how do you want to use your resources and how do you want to try and make this industry better in terms of cyber capability is really important.

This has really been about educating and informing for the most part. In 2011, we did about 200 exams looking at cyber practices. In 2014 we did a thematic sweep, and then in 2015 we put out our report on cybersecurity to provide the industry and others with our observations and what we were seeing. But of course this is a world that isn't static so the 2015 issues and challenges that were happening then, we look at a little bit differently today as things have evolved.

The other thing we're doing is we're hiring more talented and smart people in this space. It's really hard to get the right people to get asked the right questions and so in this area it's really, really important, you want to go through an exam process with smart people who understand the risks and challenges of cyber, and ask firms, observe what they're doing, test if it's working in practice and then follow up with recommendations. I think we've done that both with respect to the team that works in the sales practice area, the district offices, and with respect to the team that does all the financial and operational reviews.

I think all the things you mentioned Tim are things that we absolutely look at. One thing I think in terms of exams where we're starting to engage with firms on is insider threats. As this area has evolved a lot of firms have done a good job in "protecting the four walls,"

spent a lot of money on that, kept up to date and really looked at the infrastructure issues. But one of the biggest challenges with cybersecurity is who you're hiring and what they're going to do. I think there's a lot of good practices that we're trying to communicate through exams that develop in that area in particular.

What kind of insider threat program do you have or are you thinking about? For example there are firms that we'll monitor, badge swipes, levels, activity on printers, unusual login times, what files are leaving and I think it's critically important that people think about those things.

Another thing that's really important is what systems do you have that maintain confidential information and who has access to those systems at the firm? Is it the right people, and how often are you reviewing those entitlements? And thinking about things like that as this evolves is really, really important. So, yes, you may see someone senior at a firm making photocopies at ten o'clock at night and say that's really strange for a banker to be doing that at that level. At least you've got a red flag; you follow up and I know at least one firm found an issue with someone senior doing something like that. So looking at badge swipes, looking at activity on the computer, looking at network activity, off hours activity, all those things are important and firms have to start thinking about it, and protecting confidential information is critically important whether it's customer information or proprietary trading information. Thinking about who has access to that and even on the technology front, that's the other thing. All the people that are working on creating the code, who have a lot of access, who actually can have a direct impact to how the firm operates in a lot of ways. Focusing on all of that and looking at making sure that the right controls are in place.

I think from an exam perspective, Tim, in addition to the things that you've mentioned, these are some of the things we want to start engaging in, and again it's not to critique, it's not to write people up it's to say here's current issues that you need to be thinking about and addressing in your day to day, depending upon your work and your business model, but in your day to day business life.

Mike Pieciak:

I wanted to pick up on one thing Susan said because I think it was very important, and that is at our department, and I know a lot of state regulators and I'm sure federal regulators as well, we had to come up to speed and have to get up to speed on cyber issues as much as the regulated community or the industry. There's no reason that our examination staff had any particularized expertise in cyber issues prior to themselves making a concerted effort to get cyber certified and to become an expert particularly in the banking area where 20 or

30 years ago they might have been measuring how thick the vault was to the door, and now it's what is your software, what is your protections, what is your cyber profile.

I do think the banking industry was pretty far along on cyber issues and on the regulatory side as well for quite some time, but that work on the regulators side of making sure that you have sufficiently capable and experienced examiners is critically important.

Susan Axelrod:

Everyone wants to hire them so once you have them you're pretty vulnerable.

Mike Pieciak:

Actually we were just talking in our department about creating a specific cyber examiner that would sort of work with all of our industries and one of the points of discussion among our leadership team was if we do this and invest in them won't they just get picked up by somebody else?

Joel Reidenberg:

This is a very significant challenge for the public sector. We hear this from all the different federal agencies that have cyber responsibilities-- whether it's the intelligence services, law enforcement, or regulatory agencies-- just finding and retaining the kind of staff that you need to address the technology, law and policy problems is very challenging.

I wanted also to pick up on something Susan just said about the trend toward recognizing insider threats as significant. I thought that was especially interesting because if you turn the clock back say six, seven or eight years ago, the Secret Service and Treasury had issued reports on cyber risk in the financial services sector and the biggest threat they identified back then was the insider threat; it was a greater threat than the external hacker.

This suggests the issues are coming full circle. Thinking about the different guidance statements that have been issued over the last few years, the earlier guidance documents were framed by a sense of perhaps an external rather than internal threat. So it's an interesting reversion that's taking place. This raises a question for Tim. With respect to the insider threat and thinking about the kinds of programs that companies now are disclosing, does this threat push companies to implement artificial intelligence and machine learning systems to detect unusual network activity like a particular photocopier being used by an employee at ten o'clock at night?

Tim Burke:

Absolutely, and let me sort of preface everything by saying I'm an enforcement lawyer. I am not a cybersecurity lawyer, we have a cybersecurity group here at Morgan Lewis that is fantastic; I draw them in whenever we get an enforcement case because of the level of expertise and the technology they bring.

We all learn lessons from the enforcement cases that the regulators bring, and just a couple of months ago the SEC brought a case against a major broker-dealer, I won't mention the name but it's in the written materials that the folks have for CLE purposes. But this particular broker-dealer had an employee, I'll mention his name – Galen Marsh, who was a registered sales assistant of a major broker-dealer, and Galen Marsh was running some reports through this broker-dealer and he stumbled upon an opportunity to access literally account records for all the clients of this particular broker-dealer.

Mr. Marsh then took that opportunity; he logged in from his remote access home computer to the firm's system and he downloaded 730,000 employee records, and then he saved it onto his personal server at home. Now unfortunately for Mr. Marsh his personal server was hacked, and the records of 730,000 people were found on three internet sites for sale and apparently the sale price was ironically enough bit coin, so you could purchase customer records for a certain amount of bit coin.

In any event the SEC investigated the matter and despite the fact that this broker-dealer self-detected the issue, that they immediately disclosed the breach to any potentially affected client, and that they took the remedial measures to make sure this type of access could never happen again. And it was attributed to a programming flaw. Despite all of those steps, the firm was fined a million dollars, which is a significant penalty in the context of a firm that itself was frankly the victim of a rogue employee.

Susan Axelrod:

Well Tim what I was going to say was that case, Galen Marsh, is a reminder of entitlements, why was he able to access all that information for a firm from clients, so that's the lesson to say don't just do it once and rest on your laurels. Have some cadence by which you review who in your organization, regardless of what level, has access to confidential information and make a determination to whether or not that is appropriate. I think you're right and you raise another point -- the million dollar fine being a significant fine. I agree with you, I think it is significant, and you do hear from firms when they have attacks and they disclose it and they work on fixing it and all of us regulators jump in and say "we want to know what happened" we all make phone calls in the same day and the firm is completely overwhelmed. Most often we don't know each other is calling, but one firm once said "we are the victim here." We are the victim, we have done everything we can, we've spent tens

of millions if not hundreds of millions of dollars to protect where we are, and you guys are acting like we are the bad actor here.

There's got to be a balance and that gets back to my earlier point. The purpose of an enforcement case, the purpose of an enforcement action, it is accident deterrent, it's about message of conduct. But the education part is critically important because firms that want to get it right will work hard to get it right, they'll learn from others' mistakes. They will read whatever action and guidance is out there. And for us, smaller firms don't necessarily learn from the large firm enforcement cases, and so on our website at FINRA.org we have a page devoted to cybersecurity.

We came up with a small firm checklist for cybersecurity because again the small firms are not going to understand this big bank had this problem how does that impact me. And then we have hosted cybersecurity events, either through FINRA, through the annual conference, so we can make sure we're getting the broadest range of information out there to all the regulated advisors.

Joel Reidenberg:

I'm going to throw in some skepticism on the proposition that education is an effective way to assure better cybersecurity. When we think about the role of enforcement outside this regulated space, we have examples where education wasn't the problem. If we just look at the Equifax example, where a large company like that fails to patch a well known significant security flaw, I don't see how education efforts would work to prevent that problem for those types of organizations. Even the Galen Marsh case looking at the facts that were disclosed as a result of the enforcement proceeding, it was pretty mindboggling that that major firm was so lax in the way it's IT system worked. As you said these are firms that are already spending tens of millions of dollars on security, so doesn't there come a point where the effectiveness of hoping to educate them is simply a pipedream?

Susan Axelrod:

I think it's a case by case analysis and every case you have to look at, if the firm had complete disregard for what they need to do. Some firms say, "I'm not going to spend the money in this case." In some instances, they were aware of prior issues and didn't deal with them. Those cases are much more ripe for enforcement action. This is an area where you have to look at facts and circumstances, I think you have to look at were their actions reasonable. We did bring an enforcement case where a firm basically had an employee who left an unencrypted laptop in a public restroom and it had 300,000 client records on it. The firm knew for several years it should have encrypted laptops. That's the prefect case to bring from an enforcement standpoint. Prior notice, not reasonable action and look at the

vulnerability of 300,000 records. So I agree with you, education is not always the answer, but for an industry with this many diverse business models and sizes of firms; for an industry where there's a lot of vulnerability, education has got to be part of it because firms don't have the ability to look thematically and see what's happening the way regulators like we can do.

Sharing is preventative, but you're right it's all facts and circumstances. Negligence, not focusing, not devoting the resources is going to get you likely into enforcement.

Mike Pieciak:

The only piece that I'll add about that is why I think another reason education is so critically important is that from the smaller regulated entity area and also from a smaller business area I think the perception is, "well, I'm too small to be targeted" or "nobody wants my client information or my stuff," and whatever. It's very clear that today it doesn't matter if you have one person or a million people, or if you have one set or very small number of sensitive information, or tons of it.

If you're connected to the internet, then you're targeted and you have the possibility of having some exposure. So I think there's clearly an education component to having smaller regulated entities and having smaller companies understand that they are part of this cybersecurity threat community and that they need to be responding to it in some way.

Joel Reidenberg:

Great, why don't we move to another topic since we have a series of issues we really wanted to cover this morning – federal/state harmonization and coordination? Mike, how about we start with you, do you see the state and federal requirements as competing with each other or as supporting each other? What's your perspective on it?

Mike Pieciak:

It's a really good question because it's somewhat of an evolving issue; it's been around with us now for a number of years. You see states like Vermont, Colorado in the security space making specific moves forward in terms of requiring certain policies and whatnot. You see the State of New York moving forward in the insurance and the banking space, having their cyber requirements. The NAIC, the National Association Insurance Commissioners, in December will be voting on a final model act for cybersecurity and that will likely be implemented in a number, if not all, jurisdictions in the country.

I think there's a lot of regulators at the state and federal level that are working to sort of get out and put something on the books and to move forward and I think that's good and well,

but I think probably the next step of that progression is trying, to use the word "harmonize" to try to insure that there's not overlapping and competing requirements in these various regulations. Not all regulated entities fit clearly in one industry or another whether it's between state regulators or state and federal regulators.

One thing that state regulators and federal regulators are part of is FBIIC, or Financial Banking Information Infrastructure Committee. So NASAA, the NIC, CSBS which is the bank state regulator association, and then a number of federal regulators sit on FBIIC and they meet I believe monthly and they discuss all types of risks including cybersecurity risks.

So that's one vehicle that will help in terms of the harmonization between state and federal and even among the states as well. But I think once these various entities have moved forward from a regulatory standpoint, the next natural progression would be to ensure they're harmonized and that they work with each other and that they're not unnecessarily overlapping or competing with each other.

Susan Axelrod:

I think as regulators at FINRA and some of the programs I run I always think about constant improvement mode. How can we do better every day, and particularly with respect to cybersecurity and coordination and trying to have a single set of standards which right now does not exist. I think Mike you said it well; we have some states being active in the space; we have the federal regulators who have certain expectations; we have SRO's like FINRA and others; and there have been some attempts to have everyone think about it. I think this is an area that's right for more work, I think that if regulators have different expectations that could drive cost for firms, taking away from the real issue which is not the best result. And I think overall we should think about what works; yes, regulators cooperate, they work together they try not to duplicate cyber exams. We work with the states regularly on duplication issues, we work with the SEC, and so we all talk and work on it.

But the comment was, we get a lot of information requests, they are notionally similar but semantically different. So just by the nature of our requests we think we're all kind of getting it right, we're doing it differently and it doesn't mean we all have to have one standard set of requests. It's not going to happen with states, SRO's, federal regulators, but what we need to do is what are we trying to accomplish here. How do we request the information and handle these oversight responsibilities in the most effective way, the most efficient way and tackle the root of the problem.

From my perspective there is more to be done here and I think it's a good area. I think a lot of entities are, this is a priority for everyone. There's more we can do here; I think we do

try and work together and it's part of how we operate every day; but again it's not just states and FINRA, there's a lot of others that play in the space.

Joel Reidenberg:

So both Susan and Mike have just identified this is an area ripe for coordination and harmonization. Tim, if you could ask the regulators to focus on one or two particular areas for harmonization going forward, what would you want them to look at first?

Tim Burke:

That is a good question.

Susan Axelrod:

I may have to take notes.

Tim Burke:

It's one where you might hope that after the events of last week there'd be some regulatory empathy, now that we all know the SEC itself had its Edgar system hacked and potentially used for insider trading purposes.

I think where firms really struggle is when it comes to what are the standards expected, and we talk about the enforcement cases and the lessons learned from those, but technology breaches or lapses look obvious in hindsight. You know, how could they have not encrypted a laptop or how could they have allowed access through a programming flaw, but the reality is firms do invest a tremendous amount of resources to develop the technology, to test the technology, to keep the technology up to date and it is kind of a 20/20 hindsight standard when there is a breach and I think if there were harmonized standards at the state level, FINRA doesn't really even have a cybersecurity rule. It falls into the just and equitable rule and reasonable systems of supervision and the like.

It would be I think very, very helpful if the regulators could articulate the standards and obviously recognize they need to be kept current.

Joel Reidenberg:

Meredith, when the SEC first focused on coming up with cybersecurity guidance, was there much consultation between the SEC and other government agencies? It was probably a little before the SEC's work that NIST in the Commerce Department started working on its framework, but at least there was expertise in the cybersecurity space in other federal agencies. Was that part of the conversation for the SEC?

Meredith Cross:

I had lots of interesting conversations that I'm not allowed to talk about because the privilege still applies from back when you worked in the government. But yes there were.

Joel Reidenberg:

Maybe I phrased it poorly. What I was interested in learning was whether this kind of interchange took place, not the details of the interchange.

Meredith Cross:

So the SEC is an independent agency, and so it does what it does but at the same time we benefited from what other groups knew within the government including in the White House, in the cabinet agencies, and groups on The Hill. We definitely talked, I think it was a very early time in the process and I think there was a major concern at the time which is reflected in the guidance that you didn't want to require companies to put a roadmap into their vulnerabilities in their SEC filings. That wasn't going to do anybody any good, so there was a lot of talk about that. There was a lot of talk in the government at the time about direct federal regulation of cyber, and there were bills floating around that were pretty unrealistic because they didn't have much prospects for passing and they were going to cost a fortune and they probably would have been antiquated before they happened, and so there was a lot of talk about that.

Essentially I'd say the SEC, from a disclosure standpoint, just sort of peeled off and decided at a minimum companies should be reminded about their disclosure requirements because they exist, and the one thing nice about the SEC disclosure requirements is they exist pretty fluidly, they work for any kind of issue, you don't have to have a specific rule about cyber. So that was the purpose of the guidance; it was to get something out quickly that didn't require rulemaking, didn't require commission action; but yes we coordinate it in the sense of gathering information.

Joel Reidenberg:

Okay, any other observations on the harmonization or coordination between federal and state?

Meredith Cross:

The only other thing I'd mention on the disclosure front there isn't anything at the state level that I'm aware of and so this is something where you're really just looking, for at least for securities purposes, to the federal disclosure requirements. There's an interesting

intersection between that and the requirements in the states to provide notice to customers, and companies regularly grapple with the combination of you've got something you need to notify customers about, what do you do about federal disclosure at the time. So that's an interesting question, so there isn't harmonization there and it's just something that you have to figure out as a practitioner how to advise on. And I do want to emphasize by the way, I'm not talking about any particular company here, just as a general proposition that's something that one thinks about when you advise on this stuff.

Susan Axelrod:

I was just going to say I think that is challenging, all the reporting requirements by state. You really have to know who your customers are that were impacted. It could be hundreds of thousands, you've got to parse that out by state and then you've got to figure out what the disclosure requirements are. I do agree it's also something, we run a helpline for senior investors and we have similar state by state requirements there, and some firms need help with that and say "can you help us talk through what the requirements are" if they don't have five people to look at that.

Joel Reidenberg:

So the question is, I'm repeating it because we're recording. The question goes to recordkeeping and whether there are varying requirements for recordkeeping.

Maybe I'll ask Tim, I see you nodding your head there. This is one you're probably dealing with regularly.

Tim Burke:

Yes and it's a very interesting question because it sort of goes back to the 1996 NSMIA Act where the federal government said when it comes to matters of books and records or operational reporting requirements that's for the feds to dictate what the rules are, not the states, so we've kind of moved away from what was an intent to harmonize books and records requirements and cybersecurity is one of the areas where we've seen the states come up with differing standards and that was supposed to have been done away with. It's a blanket preemption, so I haven't seen anybody challenge a state on that basis yet, but I do think it's an area where it could be a legitimate challenge.

Joel Reidenberg:

That's an interesting one because the New York State regulation has an audit requirement and a recordkeeping requirement for future forensics. How NY decides to interpret these requirements and what exactly they mean may be very interesting.

Tim Burke:

I think it could be an interesting challenge in the future, it seems as though the states have just sort of blown right past the preemption issue.

Joel Reidenberg:

Let's turn to talk a little bit about corporate governance. Here the first question is really how have boards of directors been affected by cybersecurity? How is this affecting them, Meredith, you want to kick it off?

Meredith Cross:

I'll start it off. I think first of all it's very important to remember that boards of directors don't manage the company; they are in an oversight role and so a lot of times you'll hear people hollering about "why didn't the board do this or that" and I think the first principle here is boards oversee companies. I think what I've seen in my practice over the years is enhanced interest from the board about cybersecurity. It's an area in the risk oversight function of boards that they are certainly getting additional information about. They want to know that there's good qualified people who are reporting on it. For the most part they assign it to primarily being overseen by a committee, usually the audit committee. Sometimes a risk committee that will report in to the audit committee or that otherwise, since the audit committee has to oversee risks at least for NYC purposes, you'll see portions of the board that have it as it's primarily set in one committee. But the board will get regular reports about it and it's certainly an area that's of interest to boards.

Audit committees, to be very honest, everyone knows are overworked; there's a ton of responsibilities assigned to audit committees and boards in general have more and more responsibilities, and I think it is important to step back and look at it in terms of board oversight and so they need to make sure they've got good management and they get reporting in and they ask good questions. But it has definitely increased the workload for boards significantly.

Mike Pieciak:

I think that's absolutely right, from just a board perspective the cybersecurity IT related issues I think at one point in the not too distant past was thought of as that's for the management team and that's not a board level issue or whatnot. I think certainly there's a growing recognition that cybersecurity in particular, and cyber threats, are certainly a board level issue and boards should be focused on those issues and themselves have enough expertise to be able to determine whether their organization is doing enough in that space.

The other thing that's somewhat interesting for boards and just more generally is the shift that has happened in cybersecurity in the last year or two from really a prevention model. How do you prevent the cyber attacks from happening, how do you have sufficient policies in place and how do you have all those sort of testing and how do you have the employee training, to really a response model where there's sort of a growing recognition that it's not "if" it's going to happen it's "when" it's going to happen. I think that changes the mindset of the board as well in terms of not only do we have a plan in place to prevent it but what is our response going to be when it happens. And that second component I think is definitely something a board should continue to consider as we go along.

Tim Burke:

I'll just note on the board governance issue that Chairman Clayton has said publically that he believes that there should be a requirement that there be a cybersecurity seat on every public company board, so obviously he's envisioning something different than an audit committee role for that cybersecurity seat. I would predict that we're going to see some changes with respect to those requirements.

Meredith Cross:

I'll jump in just real quickly. The SEC will be, certainly for regulated entities, able to say what kind of people they should have on their board; it's a disclosure driven process for regular public companies and the rules that were adopted I think in 2009 that required disclosure of how the board oversees risk, have done a good job actually of getting companies to think about mapping to committees within the board where all the different risks are overseen. You've got to describe it in your proxy statement and so that has enhanced that activity, but I think it is tougher for the government to mandate any particular person on a board. So it instead kind of gets back to the skills matrix that you see in people's proxy statements. Those sorts of things so that investors understand what the issue is.

Joel Reidenberg:

Tim, you had just mentioned the chairman's desire to see a point person on the board, and Meredith you pointed out earlier that it often falls to the audit committee that's overworked. Do you think these two pieces combined are pushing in the direction that it would be – I'll call it a best practice, sometime in the not distant future for boards to have a separate cyber committee?

Meredith Cross:

I think it depends on the company and for some companies there's going to be more important issues that might deserve a committee, so I think you need to look company by company and I just don't think it's a good idea to just decide suddenly this is the issue where we need a committee. I think you could have dedicated meetings to hear about, for whatever committee it's in, to hear about the cyber issues.

One thing I think probably could use fixing is the listing standards on oversight of risk, put it in audit and then there's this exercise that goes on that makes sure wherever you assign it out to reports back into audit so that audit can see that it oversees all the risk. It would make things certainly simpler and logical to allow companies to have committees that take on particular responsibilities that don't have to report into the audit committee. I think that would be a simple change that I suspect most people would favor.

Susan Axelrod:

I was just going to add just in talking to boards and working and reviewing firm activity, this has definitely in the last five to seven years been an area of increasing focus for firms at the board level. You do see a lot of firms focusing on A) getting either cyber expertise or former chief information officers who may have that as part of their portfolio. If we were to mandate a cyber committee or a cyber seat on a board there's not probably five million people that would fit in the pool to be considered.

So I have one son who's in college and I say you should become a cybersecurity person because you'll be employed for the rest of your life – not very interested of course because it was my suggestion, but when you think about potential people who would be good board candidates whether it's public company regulated entity, having this skill set is going to be critical. So at the board level I think all board members are interested because it is a key risk as Meredith has mentioned, but if you start having a cyber committee then another issue pops up in the world we live in and "oh" do we need a committee for this.

What you don't want to do is have the issue diluted or delegated to a committee when the board members at large should understand what the firm or what the entity does.

Joel Reidenberg:

I think it's more perhaps that we're so ensconced in the information age, that information management and how we protect that information are the equivalent functions to auditing. If you turn the clock back 50 years ago on the audit function, what it was, why it existed and how it operated was critical to asset management. Today, information is the asset and the information control function has the same importance as auditing, but we are still in an old mindset and I don't think we have recognized the shift.

Let me give for those attending by teleconference so that you can receive your CLE credit, your secret code, the alphanumeric code for you to write down is: SP1993.

Why don't we turn to the topic of the future, what do you think if we were looking in our crystal balls, what might future regulatory interest look like? Where are directions that you think going forward regulators might be focusing on? In the past everyone was concerned they were one regulatory breach away from some legislative action or regulatory response; now it sounds like there's a little more strategic thinking trying to have more forward vision. Where do you think this may be leading us in the next few years?

Tim Burke:

Maybe I'll kick it off professor. We talked earlier about the inside job risk in managing your own employees. I think there's also a growing concern, growing awareness, about vendor risk, third party risk and we have seen a lot of public companies really ramp up their efforts to insure that the vendors that they're using, including law firms, are compliant with their own technology standards, policies and procedures. There were a couple of enforcement cases brought in the last year, one of which was a significant FINRA case that involved a large size broker-dealer that hired a vendor to do essentially a cloud-based server storage programming. That vendor didn't comply with the firm's policies and procedures and that led to a failure to supervise charge being brought against that firm. It was ultimately settled for a significant six figure number. But that's an area where I think we're going to see evolution both on the enforcement side as well as the internal compliance needs and governance needs. So it's not just inside your own house, it's anybody you hire to come provide services to that house.

Joel Reidenberg:

Which is essentially the whole industry, the way these services are being provided they're relying on Amazon web service, they're going to cloud service providers, they're not doing it entirely in-house .

Tim Burke:

That is absolutely right, and the smaller the company the more likely it is to use the outside vendors.

Joel Reidenberg:

Then should the regulators be thinking about leverage over the service providers? Suppose you're a small company and you're looking at who is going to host your system and your

choices are one of three organizations, large companies, we all know who they are, the small company has no leverage to negotiate any terms of that contract.

Is this something that in the future may generate conflict or regulation – if the obligation on the small investment firm is they have to supervise but they can't get a contract with a third party service provider that will allow them to satisfy that obligation, is this something we'll see coming down the pike and if so how might we look at it?

Tim Burke:

I think we're already seeing it, the SEC brought a case against a small RIA firm, again it's in the materials for the details, but that firm hired an outside service to provide exactly what you described, the type of data storage that they couldn't do in house. The outside server was hacked, and the firm did what you would expect a responsible firm to do. They went out and they hired multiple cyber forensic firms, those firms concluded that yes there was a hack, it appeared to have come from mainland China IP addresses, but there was no evidence that any customer data was actually accessed through that hack or that any customers actually were harmed in any way. This is in the SEC's release and SEC acknowledged that, but they still fined the firm and the grounds for fining the firm was essentially that the firm didn't have adequate policies and procedures to do the kind of testing on the third party vendor. So it wasn't a strict liability standard that you're responsible for the acts of others but it was more of a did you have adequate internal procedures to at least be asking the right questions and doing the right testing.

Susan Axelrod:

I was going to say the third party vendor issue is a key issue and I think in the past couple years it's been an area we've been fairly vocal on to say you've got to know who you're hiring, you've got to have procedures in place, you've got to ensure they comply with your standards and you've got to have some check and balance to make sure that's actually happening. I think, and Tim you said it, but I was going to say perfection is not the standard. It cannot be. But there's got to be adequate or reasonable oversight of the vendor to ensure they're complying with the firm's policies and procedures in this area.

Understanding it is a challenge; the adequacy of what a firm does I think will define their fate when it comes to these types of issues.

Joel Reidenberg:

Mike, do you also see the practices of third party vendors as the key issue coming down the pike or are there other issues you would imagine?

Mike Pieciak:

I do, when you think of the issues that Susan identified, the insider threat. I think unfortunately employees remain, individuals remain the greatest weakness for companies, whether it's an insider threat or it's just a lack of training, a lack of knowledge. The classic phishing email, the ransomware attacks that come from that, those are on the rise and morphing and changing on a daily basis once they're identified, particularly real estate attorneys are dealing with this as well, or even anybody that is holding cash for clients and sending out disbursements, sending out wires. They are so sophisticated sometimes that you're just amazed that they understand there was a deal that was closing on X-Day and they come in right at the appropriate time with a phishing email that says, the wires have changed here's the new wire instructions, and whatever give me a call if you need anything. The email is the person's email that you would expect to send such a message, so threat is always evolving and I think that's on a number of fronts. I think it's going to be continued response from regulators, but I also think there is and is going to continue to be a response from the business community from the corporate community because people do not want to be an Equifax or an Anthem or a Target or whatever. They don't want to be the next example and have the bad publicity that happens with that.

As I mentioned it's becoming much more, it's moving from that prevent to sort of that recovery and response mindset, but at the same time I think there's a lot of reasons for companies to take this very seriously and to progress forward.

One example I'll give that happened in Vermont a couple of months ago and where you see this going and why I think it's so important to have a response mindset. There was a small electric company in Burlington, Vermont, one of its computers that was not connected to its network had a malware that was from Russia and there was a great concern all of a sudden that this was connected to the larger grid and that this might be a way in to our electrical system nationally. I can tell you that the CEO of that company was inundated for a day and a half, two days, with so many inquiries from press, from regulators, from politicians, from government people and I would be that they now have a much different type of cyber response plan than they did maybe a year ago.

When you're in the morass of trying to figure out what happened, how to respond and then taking on that sort of external inquiry can be really challenging. So I think that's why it's important to have that response plan and recovery plan.

Susan Axelrod:

One thing I was going to say also that I've seen change and will continue to change is consumer or customer response to all this. Years ago we all were dealing with a "hi, this is

Susan I'd like $2,000 transferred from my account, I'm on a plane I'm going to London I won't be able to talk to you when it's landed, I need this done." Years ago someone would say I've got to do this, she's a good client I want to get it done, I don't care about calling back, I don't care about getting confirmation somehow. People were doing things to accommodate customers, because customers were demanding it. You would hear multi-authentication logins, our clients do not want to have a really complicated password that they won't remember. They don't want to have to login to two systems.

There were a lot of firms reacting to what their customers, what their investors wanted in terms of ease and convenience. This whole environment I think has changed consumer expectations. People are willing to get to that phone call or send that confirm in writing that they want money transferred. Customers are willing to say yes I want to have multiple logins because it's protecting my account. So I think there's been an evolution in terms of convenience and moving forward versus the current environment and we have to have checks and balances both from an internal perspective and consumers have to be willing to do that.

I think that has been very positive because everyone is kind of in this together. We want to do the best we can for individual assets, information at a corporate level and for our country as a whole.

Joel Reidenberg:

Yes. Let me turn to one final question. What's the one takeaway message that you would give folks today about cybersecurity looking toward the future, from today's session what would be your takeaway? Meredith, we'll start at your end and just work toward me.

Meredith Cross:

I expect that the Commission will come out with enhanced guidance or rules or something to beef up their expectations with regard to cybersecurity disclosure by regular public companies. Chairman Clayton said it in his testimony in congress whenever that was, last week, and I expect that is going to be a high priority for them. It's not surprising that this change is coming but I think people should expect to see additional guidance from the SEC on this.

Tim Burke:

I would say, and this has been amplified in both the SEC and the FINRA exam priorities, but the tone from the top of an organization I think is very important. It's critical for senior management to emphasize the policies and procedures and the need to continually test and validate those procedures, and if an organization does have that tone from the top message,

I think that really does help when you're defending a company that has been victimized by a cybersecurity attack and demonstrating to the regulators that these things are going to happen. We had adequate policies and procedures; we acted reasonably and here's the best example we can point you to; this is what our president or CEO has done with respect to these issues.

Mike Pieciak:

Yes, that's a good point. I think my takeaway is really somewhat of a no-brainer which is that cybersecurity threat is pervasive, it is impacting everyone from the smallest to the largest companies. It's not going away any time soon and I think it's going to continue to grow and even become more prevalent which is unfortunate. And again this is the third time I've mentioned it, but really the prevention model is somewhat becoming antiquated and it's becoming much more of the recovery and the response model. I think there will become a growing – acceptance is not the right word, but there will be a growing recognition that it's not "if" but "when" in terms of both big and small companies.

Susan Axelrod:

I was going to copycat a little bit of what Mike said because I do think no organization can predict that they don't have vulnerabilities. And with the rate of technology change that occurs and our dependency on technology this is a real threat every day, it's not just for financial services but for other organizations as we've seen. It'll be interesting to see the reaction from a legislative standpoint at the federal level if there's anything that results from the events over the past three weeks, and again we'll all watch and wait and see in that space together. But I think the most important thing to do is focus on this area, stay on top of current trends.

When I heard that some folks were calling you on your phone recording your voice and then using that to do other things I mean it's hard to believe you don't even want to pick up your phone when you don't know whose calling. The blocked or no ID, those things, I don't even pick them up anymore. So trying to stay on top of what's happening and think about ways, you won't be able to prevent it, it's the when and not if, I think as Mike as said. But I completely agree having a plan in place, not just relying on your standard business continuity practices, thinking about your public message, the communication with customers and how you would work through potentially any denial of service and attacks. All of that is critically important because perfection can't be the standard for all of this, but thinking through what the plan would be, what the message would be, how you would deal with the regulators and how you'd make sure you'd be able to do your business is critically important. I can't agree more that's one of the best things forward looking that I think we can recommend to firms is be thinking in that mode not we've got to cover.

Joel Reidenberg:

So I am walking away with a historical takeaway message actually. If we look at where we started-- how the SEC was first getting involved in cybersecurity-- and some of the points we've just reached about vendors, the pattern that we're seeing I think quite clearly is that the expectations are constantly rising. The expectations for what an organization needs to do change because the risks change and these risks are increasing and are not going to decrease. This suggests, at least to me, that cybersecurity is something for very, very careful and continuous board of director's attention. The culture of organizations, whether a small organization or a large organization, follows from the board down to the implementation level of the organization's plans and strategies. Because each of the enforcement cases we heard about were ones where implementation didn't happen and the education portion needs to be driven from the top.

It seems to me if we look at this historical pattern the expectations and standards will constantly be rising for corporations.

As we come to the end of our discussion, I would like to thank Mike, Meredith, Susan and Tim very much for sharing your insights. I hope that the audience here in New York, listening online, or via teleconference found it to be an informative discussion.

As an academic it was fascinating for me.

The program we expect will add to the valuable body of knowledge in the series. The video broadcast will be available soon in the Virtual Museum and Archive, an edited transcript will be added later.

On behalf of the SEC Historical Society I would like to thank Morgan Lewis again for the sponsorship and their hospitality in making today's program possible. Thank you all for joining us and have a great day.

END