Julia: **Hello and welcome to DerivSource podcast. I'm Julia Schieffer, the founder and editor of DerivSource.com.**

Cyber risk remains a mainstay in global news as there is a steady stream of news of website and email hacks. And recently the FDIC, OCC and FRB announced enhanced cyber risk management standards for financial institutions in the form of an advanced notice of proposed rule-making.

In this DerivSource podcast we speak to Harriet Pearson, partner and head of cybersecurity practice at Hogan Lovells in Washington DC and New York, to explore the potential enhanced cyber risk management standards proposed by these three federal banking regulatory agencies in the US. And we'll also explore how financial firms should be bolstering their cyber security measures today.

Welcome to the podcast Harriet.

Harriet: Thank you Julia, I am happy to be here.

Julia: **So Harriet, can you first give our audience a little bit of background into yourself?**

Harriet: Sure. I am a partner at a law firm called Hogan Lovells, where I lead our cyber security team and co-lead something we call *cyber risk services* - a consulting unit. I have been practicing and working in cyber security and data privacy for about 20 years now, and spent a lot of years at IBM, where I was Chief Privacy Officer and Security Counsel there, before joining Hogan Lovells in 2012.

Julia: **You are well equipped to talk about cyber risk.**

Harriet: I've had a number of years in this areas, even before they were called *cyber,* or these other terms that we are using these days. So yeah, I've got operational as well as legal and compliance experience.

Julia: **Fantastic. Well, let's start about what's been going on with news so far. With website and email hacks and news constantly now, what is the real threat of cyber risk to financial institutions?**

Harriet: Well, there is no one *threat* and the reality is that there is a reason that regulators and others are focused on the programs that are in place in financial institutions. We have to worry about all of this. Cyber security risk is not really just one thing; there has to be a focus against website attacks and the kind of very public events that happened in the last several weeks, and that had been noted, because those kind of website attacks can distract or worse, they can interrupt business operations in the way that is maybe annoying, maybe a nuisance, but actually it can be over time quite damaging if it's not dealt with.

But importantly, you also have to guard against insider attempts or more sophisticated attempts to compromise systems in the way that will potentially divert funds, tamper with accounts or even affect operations more deeply. So, the real threat, I think, to financial institutions of cyber security risks is the fact that its multifaceted and requires a lot of attention and a constant reprioritisation to make sure that the right threats are been addressed and that the right resources are deployed.

Julia: **So clearly people have to keep on their toes as this is a very much an evolving space.**

Harriet: It's an evolving space. Addressing cyber security risk is a team sport. I know listeners to this podcast are of different backgrounds and different discipline. You may be a compliance person, an a risk manager, an IT leader, a lawyer... Frankly, all of those disciplines and more are involved in addressing cyber security risk. I believe that strongly - I've seen that in action. That's the only way really we can make it though what unfortunately is a very challenging area.

Julia: Now, recently the FDIC, OCC and FRB announced enhanced cyber risk management standards for financial institutions in the form of an advanced notice of proposed rule-making (ANPR). So, Harriet, can you briefly outline these standards, and explain what this means to financial institutions?

Harriet: Yeah, I am happy to give an overview of this joint notice of proposed rule-making that was published on October the 19th in the United States by those three major banking regulators.

First and foremost was the notice of proposed rule-making, so it's the beginning of what probably will be a fairly length process. This is not an overnight regulation but it is an important signal that what is likely to happen is that more cyber security regulation is coming to the US financial sector and to the largest and most significant financial institutions.

The ANPR has 39 questions posed. 39 questions to which it's asking for answers or comments which are due January 17 of 2017.

The intent of the notice of proposed rule-making is to obtain input from all interested stakeholders on what these enhanced cyber risk management standards should be.

The covered entities for the enhanced standards are going to be (at least according to the rule-making) are supervised institutions with over $50 billion dollars in assets, firms that are going to be considered sector-critical because they're very, very important to the functioning of the system, and service providers to those kind of firms (sector-critical firms as well as the supervised institutions with more than $50 billion dollars in assets).

So, importantly, any vendor, any service provider that serves these organizations also would be covered here.

The notice of proposed rule-making would create… I think what the intention of the regulators is to create mandated standards. There is a lengthy discussion in the ANPR of all the different regulatory and guideline types of documents that exist today that inform and already really, frankly, regulate this industry and this sector. So this is something that is intended to be *enhanced* and *additional* to what's already there. Read between the tea leaves, it's intended to create a mandatory baseline and the ANPR is stressing our five different areas of cyber risk management.

Number one is: They're looking at cyber risk governance and asking questions about what could most effectively be done to engage Boards of Directors to ensure that they have the right expertise to oversee this kind of risk? I think if these enhanced standards get enacted the way they're being posed, you'd see a lot more expectation (a higher expectation) for Board engagement, awareness and expertise in this area.

The second area that the enhanced standards board address is risk management, stronger risk management, and I thought the most interesting aspect of this particular section of the ANPR is the idea that there would be three mandatory functions inside a company that will provide the cyber risk lines of defense. 1) Mandatory audit function; 2) Mandatory IT security, program or function; 3) Mandatory Chief Risk Person or Officer who would be responsible for reporting to the Board and perhaps to the Chief Risk Officer overall on cyber risk management.

Many institutions have these three functions, but many do not at the moment, and so this would really drive I think the emergence of a more strategic risk management function that’s focused purely on cyber security in addition to the core IT security functions that exist of course in all financial institutions of size.

The third area in which the ANPR focuses and asks questions is something they call internal dependency management. That’s a pretty interesting term. What it really means is that they’re focused on what kinds of essential elements should be in a mandated security program. Things like making sure you have accounting or inventory of all assets under management, and I’m talking now about IT assets not financial assets. Having a strong internal program that is about the systems management, security, policies, procedures, all of that, the kind of programs that a typical IT security team would run, this is a focus on that.

The fourth area is external dependency management, and this is all about the ecosystem in which the covered entities operate. Ecosystem including e-service providers, partners, and the idea here is taking vendor oversight and third-party oversight to a place where there would be mandated enhanced standards for that.

The fifth area is around incident response, resilience and situational awareness, which just to put that in plain language means “do you know what’s going on around you, as an institution? What are the threats, who’s after attacking your organization or sector? Are you ready to respond to that so you can power through and return to operations in a normal way as soon as possible?”. And there are questions about how best to impose or develop and provide enhanced standards in that area.

That’s the core of the ANPR and separately from this core inquiry there’s also an articulation of desire to have even more stringent standards for so-called sector-critical entities. For example, for those particular entities a requirement to implement something the ANPR calls most effective commercially available controls, and that is a moving target at any one moment, and it establishes a really high bar that I personally in my practice have not seen articulated anywhere else for any other sector. Most effective commercially available controls, as opposed to reasonable practices, or industry standard practices. This is a really high bar.

Another example of what would potentially be applied to sector-critical entities is to establish and validate that you can return to operations in two hours once you’ve been hit, if you’ve been hit by a cyber attack, which is a very, very short timeframe indeed, but understandable potentially if you’re talking about entities that are truly sector-critical.

All of the above, everything I’ve talked about would cover and apply to service providers, which is why I think this ANPR is of interest, obviously not only to the core covered entities in the sector but also to another, wider ecosystem.

Julia: **So, Harriet, the proposed rule-making sounds quite extensive but as you pointed out it includes the requirement for sector-critical entities. Is this perhaps going too far? Is this needed, given people already have guidelines?**

Harriet: As you say, there are extensive regulatory requirements and detailed guidelines that are applied to this sector, to the largest institutions and to other participants in the sector, and so I suspect what we'll be seeing in the comments that will be filed by January 17th is a number of industry participants saying wait a minute, we've got standards, we just need to get support from law enforcement to prosecute cyber criminals. We need to get government support of other types, and an additional layer, or multiple layers of mandates is not exactly what is needed.

I think this will be a tension point, and you can kind of see why that would be. Technology and cyber threats move very, very quickly. Traditional notice of proposed rule-making is going to take some time. I think important for me to mention that the ANPR recognizes and leaves open whether these enhanced standards would be guidelines or would be actual mandates that take the form of detailed regulation.

I think the jury is out on that, as they say. It's an open question and I think industry participation, others' input into this process will be important. As well, I think it should be noted that with the change in our executive branch, i.e. the election of Donald Trump to the presidency, there may be some effect of the leadership of our government on how financial services regulators proceed in this area.

It's worth taking that into account here that these may not exactly be mandated by regulations, but I think the trend here that is important to note is more focus on getting more specific on what's expected from the largest institutions and their service providers just because of the risk of cyber attacks to disrupt the financial system.

Julia: Perfect. So the main takeaway here for our listeners is get those comments in by January.

Harriet: Yes. I think there's an opportunity here to shape and inform. Clearly there are 39 questions posed in the ANPR, and the more information that's submitted for the public record the richer and more influential it will be on shaping the outcome of this process.

Julia: Harriet, let's switch gears a little bit. We've talked about the proposed rule-making, but let's talk about what happens today already. Hogan Lovells has a cyber risk service already in operation that you service multiple clients. Can you briefly describe this service, what's included and how you currently help clients tackle the possible risks that we've outlined?

Harriet: Well, thank you for asking that. We're not typical lawyers, I think. We combine a team of lawyers with very deep regulatory expertise and operational experience with attorneys who are experienced in enforcement matters and litigation with a business unit called Cyber Risk Services where we have former Chief Information Security Officers of very major corporations and other consultants who are really hands-on and understand risk management and technology management in this area.

We combine our forces, so to speak, to help clients assess their governance, their compliance, develop training programs, and also in the event of a cyber event or incident we get in there to (in a very informed way) oversee any forensics and we speak the tech-talk and we speak security-talk so we're able to get really deep and then come back and explain to a Board of Directors, to General Counsel, to CEO and Compliance Officer, what has happened, what are the options and what can we do to move forward.

We are global and we have combined our tech regulatory and all the other legal disciplines into one package. We work with companies of all sizes and in all sectors including, obviously, the financial services sector.

Julia: **Given you have this Cyber Risk Services that obviously covers all the different elements you mentioned: technology, regulation etc, in your view what are the basics of a cyber risk prevention program that financial services institutions should be adopting today?**

Harriet: In my experience most financial institutions have pretty sophisticated programs, but it's always good to do a double check, that you see the forest in addition to the trees. At the forest level, if I can say it that way, it is essential to make sure that the governance of these programs keeps up to date with expectations. Is the board appropriately engaged? Does it have enough expertise at its disposal to assist it? The C-Suite, are they engaged? Do you have the right leadership in place whose skills are keeping up with what is expected in this area? Is there a strong core program, an IT security lead and a program that is appropriately resourced, given what we know today? That's going to change tomorrow, and the day after. Unfortunately, it's a moving target.

Training and awareness, or what I prefer to call building a security culture, is essential and sometimes gets overlooked. We can see in the news constantly with examples of very major organizations that get infected or compromised because somebody has done something that really could have been prevented with some training and some reinforcement of what good behavior looks like.

So a strong focus on training and security culture, which typically draws on different skill-sets, frankly, then IT security. You need people who understand culture, training and human psychology for that.

Finally, a focus in sophistication around being ready and being aware, and these are incident response planning exercises to test your capabilities. Constant testing and constant scanning of the environment.

Those are in my mind essential elements for any institution and I would add to, especially in the financial services sector, third-party, third-party, third-party oversight and unfortunately what we also have in this sector is a deep, deep attention to regulatory compliance and maintaining those good relationships with your core regulators who are expecting a constant flow of information. Having the sophistication to keep up that interaction and relationship and compliance activities with regulators while also running a program that is constantly evolving - that's not easy, but that's what I see as essential.

Julia: **We started off the conversation by talking about how cyber risk is increasing and obviously there's a clear need for firms and all different types of companies to address this. Looking ahead, how do you see, and do see, cyber risk being a growing area of concern and risk in 2017?**

Harriet: This issue is not going away any time soon. I have been working in this area literally since the late 90's and I've seen it develop over the years and I think we're just getting started frankly in terms of what will need to be done with respect to processes, technologies that need to be evolved, adapted and deployed, and the actions we all must take.

2017 and well beyond we are going to be talking about this and focusing on it as all types of professionals. This is an unfortunate facet of our reality but it is one that will be with us for quite some time.

Julia: **Thank you Harriet for sharing your views with us, it's been very insightful and no doubt our listeners will welcome the information that you've provided on this topic.**

Harriet: Thank you very much, and we have actually additional resources available if anybody is interested. Go to hoganlovells.com/cybersecurity. We have also have a dedicated site helping to test incident response plans, you can take a diagnostic there at hoganlovells.com/readysetrespond.

Julia: **Great, we'll definitely include those links on the podcast notes page, so do look at DerivSource.com for direct information on those links that Harriet kindly provided us.**

Thank you again Harriet for joining us on this podcast and for sharing your insight with us today.

Harriet: Great, thank you so much.

Julia: **Thank you to Harriet Pearson of Hogan Lovells for sharing her views with us today in this very insightful podcast. No doubt our listeners will welcome the information provided on this topic.**

We will make the links Harriet mentioned available via our podcast notes page on DerivSource.com, and if you liked this podcast please subscribe to it on iTunes or listen via our free DerivSource app or via DerivSource.com.

Thank you for tuning in, join us next time.