Fed Unfiltered, Transcript
10/6/22 – Neel Kashkari, Interview: Cleveland Fed, Cyber Risk and Financial Stability

Neel Kashkari:

Good afternoon. My name is Neel Kashkari. I'm president of the Federal Reserve Bank of Minneapolis. It is great to be with you. I'm here today to have a conversation with my friend Jay Clayton, the former chairman of the Securities and Exchange Commission. Thank you, Jay. Thank you for joining us this afternoon.

Jay Clayton:

Thank you. It's great to see you.

Neel Kashkari:

Great to see you. So just briefly on Jay's background. I don't think you need an introduction, but I'll just take a moment. Obviously, you were chairman of the Securities and Exchange Commission from 2017 to 2020, in that you worked on financial stability issues as part of the President's Working Group, the FSOC, a number of other international committees. Prior to that, you had a long career at Sullivan & Cromwell, one of the prestigious law firms in America. And you were also chairman of the cybersecurity group there at Sullivan & Cromwell. And you're now back at Sullivan & Cromwell in your post-government service. But you also have a number of other private sector roles, including being a non-executive chairman of Apollo Global Management. And you're advising many different private sector firms. And I know that cyber comes up a lot.

Neel Kashkari:

When I was talking with the organizers of this conference about what they hope to accomplish, they said that the purpose of this conference is to help senior banking executives and their boards of directors come up to speed on cyber issues and help make sure that they're at the forefront of managing and understanding their own cyber risks. So when I thought about who we might reach out to in the private sector to give us some advice, you were at the top of my list. So I really appreciate you joining us.

Neel Kashkari:

For this conversation, I thought about starting at a very big picture, which is how do you think we're doing as a country in responding to the evolving cyber landscape. And then focus on the public sector, your time at the SEC, my time at the Fed, what did you learn at the SEC, both about the sectors and the companies that the SEC oversaw, but also the SEC itself. And then third, I thought we'd go into the private sector and what advice you have for financial institutions and their boards of directors in how they think about managing their own cyber risk.

Neel Kashkari:

So with that very brief setup, I know we have a lot to cover and not a lot of time. Maybe we could start at the national level. How do you think we're doing as a nation in responding to and preparing to defend against cyber threats?

Jay Clayton:

So Neel, I think it's a great question because it is a national issue. I mean, we really framed it well. The panel before us, I had a chance to catch it. One of the themes was cybersecurity is a team sport. And the team here is a big team, 320 million people. How are we doing? I think we're doing a lot better than we were five, six, seven years ago because there is a recognition of a lot of things. One, how interconnected

we are from a cyber perspective. And because of all of those interconnections in our daily lives, the things we rely on, we're at risk. If those networks break down, how we interact with each other breaks down.

Jay Clayton:

I'm not telling you anything [inaudible 00:06:42]. But six, seven years ago, I don't think there was a recognition in the general public or frankly in a lot of boardrooms, I think financial services were ahead, that that was in fact where we had come. So now I think we have a better perspective and that better perspective has enabled us to do better as a financial services industry and more generally, and as regulators. Regulators are always looking for simple solutions. Networks often don't provide the opportunity for simple solutions. But I would say on our cybersecurity journey, we are making progress. We have a long way to go, long way to go, but we're making progress.

Neel Kashkari:

Great. So let's shift a little bit and think about the public sector for a moment. So at the Fed, and I know this is true for the SEC, we care a lot about cyber because we oversee financial institutions and critical financial infrastructure. We want to make sure that the financial institutions that we oversee are managing their risks and understanding their risks appropriately. But we also recognize that we are a target and we would be a very attractive target to bad actors around the world. So we invest a lot of money and we have a lot of talented cyber professionals helping to protect our own systems here, which are critical to the US. I know those same ideas and concerns are true at the SEC. And I know you had a firsthand experience when you got to the SEC. Maybe we could talk about your experience at the SEC as it relates to cyber.

Jay Clayton:

Sure. And those risks are not just risks in theory. They're risks in practice. And we faced that at the SEC early in my tenure. It became apparent that over time foreign actors, actors from I believe the Ukraine and contiguous countries, had hacked the SEC disclosure system. Not only had they hacked the SEC disclosure system, they managed to do so in a way that gave them access to nonpublic information and they in fact traded on that non-public information. So the hack went right to the heart of what the SEC does, which is protect markets.

Jay Clayton:

You can imagine when that came to my attention, your heart stops. What did we do? I don't know if we did it perfectly, but I knew that it was important to be as transparent as quickly as possible. And this is something that... Look, you don't know minute one the extent of the hack, what happened. These things are going to take time. But at some point fairly early on, you need to let the public know, your constituents know what has happened, what was at risk.

Jay Clayton:

So that's what we did. I actually asked for a hearing in front of the Senate Banking Committee, explained what happened, and tried to take it as an opportunity to make people aware that this type of, what I would say is commercially oriented opportunistic hacking was very prevalent. And if it could happen in the SEC and we had a decent sort of cybersecurity posture, I think it improved measurably after that, it

could happen anywhere. You talk about a real wake up call, not a theoretical wake up call, that was what.

Jay Clayton:

And then as you know, and I think you and your colleagues do a good job at this, at the FDIC and at the FSOC we went through sort of tabletop exercises. And what comes out of that is you quickly learn, as we did with our [inaudible 00:10:15], that all of the federal financial regulatory agencies are connected in any kind of large-scale hack because we have joint jurisdiction, joint responsibility. And those exercises are very worthwhile.

Neel Kashkari:

And did you find... Was there a good... Sometimes there can be competition, maybe friendly competition among agencies. Was there a willingness to share and collaborate or did you have to break through some bureaucratic barriers to get everybody on the same page and aligned?

Jay Clayton:

Yeah. I don't want to say that there were bureaucratic barriers, but that topic that we just discussed, which was the need for cooperation was not something that was as well recognized as it would've been without the exercise.

Jay Clayton:

Let's just say for example, we have a hack at a broker dealer, but that broker dealer at the SEC is sort of connected to the clearing systems or connected into a money center bank. The primary regulators or those entities, they need to know that they may be at risk due to some interconnection between the broker dealer out of pure SEC regulation. And an entity that's primarily regulated by the Fed and of course any kind of national security type issue around that, the treasury and the like. So I think over time there's now much greater recognition of how much we need to communicate among the regulators in any kind of significant cyber event.

Neel Kashkari:

And do you think... One of the things that I've observed here at the Fed is we try to... The banks that we regulate, the bank holding companies, there's a whole different set of skills that we need when we're trying to look at it through the lens of cyber risk as opposed to traditional credit risk as an example, which we're much better at and have a lot of experience. When you thought about the skills at the SEC, did you have to say, "Hey look, we need to beef up our skills in this area for our own protection, but also for the financial markets that we supervise"?

Jay Clayton:

Yeah. I think that's exactly right because you're conditioned, rightfully so, to look at the risks that you're charged with. And some cyber risks due to these network effects are actually new to the financial regulatory system. And I think that you needed to develop, in particular what we just talked about, that ability to talk across agencies, get out of the [inaudible 00:12:57] intrusion, get the information disseminated. And that took a change in mindset.

Neel Kashkari:

Yeah, I can imagine. And one other question about your time at the SEC, as it relates to the SEC, and its something that I struggle with here and I imagine leaders of organization of all stripes struggle. How do you know if you're doing enough? There's no limit to what you can do. You can always do more. You can always hire a few more security professionals. Obviously, you can't do that forever. At some point you have to give yourself confidence that we're doing the right things. How did you think about are we doing enough when you were there?

Jay Clayton:

Well, I think I'm a big believer in public-private sector communication, especially around these things. And one of the things is, okay, take one of... I don't want to pick a name, but take one of the international financial institutions that we all regulate. It's okay. In fact, you'd be crazy not to as an agency head having a dialogue with their cybersecurity teams to find out what threats they're seeing.

Jay Clayton:

Now we've set up some formal, what I would say is public-private communications channels. Very good. But having my people... I told my people at the SEC, you should feel comfortable to talk to the cybersecurity professionals in the private sector. That's not the same as talking to somebody who's has a deep commercial interest in a particular policy position. This is much more about the team sport attitudes. And I think that that's very important.

Neel Kashkari:

Yeah, good point. So let's shift and let's think about financial institutions. You've been advising financial institutions for literally decades. You continue to now. When you think about... And there's going to be a range, right? The big global firms are going to have deep benches of cybersecurity experts. But you also have smaller firms that are also attractive targets and often case because they don't have as rich bench of cybersecurity experts. What advice do you start with when you're talking to a board of directors about the role of a board of directors and what they should be doing to make sure that the firm is taking the precautionary steps that they should be taking?

Jay Clayton:

Yeah. I think people have different ways of articulating how they see a board's role. Now boards have fiduciary duties. They are there to represent shareholders and other constituencies and be there. I like to say it's really a twin role. It's oversight. Are we asking the right questions as management thinking about various things, as well as empowerment? So it's one thing to be asking a lot of questions about cybersecurity, which you should do. I don't think any board of directors can be the expert body for cybersecurity. It is an oversight role, not a management role.

Jay Clayton:

But also be empowering. It's okay to bring in an outside consultant that does penetration testing and other types of testing. It's okay to sort of spend some money to go out and I would say benchmark your cybersecurity efforts against others. It's okay to engage with the regulators around cybersecurity. Everybody looks at engaging with regulators has always involving some risk. I think this is an area where the board can say, "You should be doing that. You should be doing as much you can." So it's oversight. There's a lot of focus on, is there a cybersecurity expert on the board? I'm sort of agnostic on that. I

think you can bring people in, knowing that it's an issue, knowing it's an issue. But empowering management to actually dig in on the issue, I think is also a big part.

Neel Kashkari:

And what do you think about... The last conversation touched on this for me. Imagine there's going to be a range of views on this, which events should a board of directors and a company say, "This is something we must reveal," versus "Hey, these are minor events and we don't need to blow this out of proportion"? It seems like that's a judgment call. I'm just curious if that comes up in your deliberations with boards.

Jay Clayton:

Sure. And it comes up in deliberations with management teams as well. I believe there's some confusion in the marketplace about this. So materiality in these sort of SEC sense, we should be disclosing material events. That's material to the operations performance prospects of the company. There are lots of cyber incidents that are not really going to have that kind of effect, including in many industries because there's a cyber [inaudible 00:17:52] every moment.

Neel Kashkari:

Yes, exactly.

Jay Clayton:

And you do have to differentiate. That's a very good lens. I think that sometimes gets confused with what kind of disclosure do you want to be making the regulators want, should regulators be requesting in order to assess the overall cybersecurity posture of an industry? Or from a national security perspective, what kind of disclosure should people be making? We have tended to confuse those questions. The investing marketplace doesn't need to know how many threats, how many you had and the like. But that may be something that national security officials knew, the Fed would like to know for trends and other things like that. Those are two... And we should think about them differently.

Neel Kashkari:

And I would add one. That makes a lot of sense to me. I would add one in terms of your customers and what are your customers going to want to know. Even if it's not material, there may be certain things that they want to know just to give them confidence that you are a trusted partner and you're not going to just bury all the bad news. So, I mean, I think it's going to be pretty case specific.

Jay Clayton:

Yeah, absolutely. I mean, I can see instances where it is absolutely the right thing to do, to contact your customers whose information has been breached. But it may not be something that rises to the level of a securities law disclosure. And understanding the context of the issue I think is important.

Neel Kashkari:

Yeah, that makes sense. So let me shift gears. Central bank digital currency has gotten a lot of attention. The Fed has said that we're studying the potential. Some have suggested that there are great promise from a central bank digital currency. Some have suggested, "Hey, this could introduce new risks." And then of course you've got private sector digital currencies, like other cryptocurrencies, that may have

their own cyber risks. I'm just curious, I know that you've spent some time studying these issues. Do you have any high level views on digital currencies, central bank digital currencies specifically as it relates to cyber?

Jay Clayton:

Sure, I do. I do believe that we benefit, particularly benefit from a lot of things in the United States. We benefit from dollar hedge money, dollar being the reserve currency and something that we want to preserve. So not only do we not need to put the dollar at risk, but we also need to make sure that the dollar does not become antiquated. And so embracing technology, very important.

Jay Clayton:

What else do we have? We actually have many large banks by comparison to any other country. That makes, as I like to think about it, instead of single points of failure, much more distribution of risk. Not only around things like capital that we worry about every day, but also around systems. One thing and [inaudible 00:20:59] people who tell me about a central bank digital currency, they would be administered in a single hub by a government entity. That to me has a much different risk profile from continuing to use what I would say is our robust network of regulated and unregulated institutions to handle dollar denominated payments around the world.

Jay Clayton:

So that's kind of how I look at it from a cyber risk perspective. I think that network with multiple players and multiple nodes somehow must be better from a cyber risk perspective than introducing a closer single point of failure.

Neel Kashkari:

Yeah, that makes sense. So some way capture the benefit of innovation but not give up the resilience that we have by having this distributed system with lots of different players.

Jay Clayton:

Absolutely. Tremendously well said. And I think sometimes innovation comes from competition and figuring out a way to turn those parties loose to compete for a better way to run the rails. As I always say to people who used to come into my office at the SEC who had an innovative idea, I said, "Let's start with this. Show me how we can do our job at least as well. Reduce risk and no way increase risk and capture the innovation. And then we're going to have a real conversation. But I'm not going to trade financial stability risk, customer risk or efficiency. It's got to be at least neutral. Hopefully it furthers the mission and add efficiency."

Neel Kashkari:

In your description, you talked about, there's the banking sector. You also mentioned the non-banking sector where there's been tremendous growth over the last decade. A lot of innovation. As we are going through a policy of tightening monetary policy, you're starting to see some cracks emerge in the global economy.

Neel Kashkari:

A couple weeks ago, pension plans in the UK came under some stress because they had some interest rate risk that they may not have fully appreciated. I think it's expected that as central banks around the world continue tightening, additional cracks are likely going to show up, and they may well show up in the non-bank sector where there's less regulation and less visibility.

Neel Kashkari:

As you think about cyber risk in the heavily regulated banking in traditional sector versus the non-bank sector, is that something that gave you a lot of concern when you're at the SEC or gives you concern today about potential risk, cyber risk that are brewing in those less regulated parts of the markets?

Jay Clayton:

It's a terrific question and I think it's related to your premise. Your premise is are there pockets of risk that have the potential for systemic effect? So you mentioned [inaudible 00:23:51] too much leverage, unseen leverage, liquidity transformation that I would say is unreserved against things like that. Are there places outside of the institutions that you oversee every day where a cyber incident can have that kind of effect?

Jay Clayton:

It's more, to me... Let's say a broker dealer that is small is somehow connected into a larger financial system. That risks bothers me if it's a method for inclusion more than sort of the capital things that I think we've... Let me put it this way. There's been, as you mentioned, some UK turmoil. I think most people you talk to still consider the risks, but know that from a capital and liquidity perspective, we're a much better position today than we were in 2007, 2008.

Neel Kashkari:

Let me repeat it back to you in my own words and see if I capture the spirit of what you're saying. And that is say some small hedge fund is exposed and gets hacked, that's probably not going to be destabilizing for the US financial system as opposed to a broker dealer that is much closer to the center and is connected to a lot of other financial institutions. That potentially is riskier in terms of cyber risk spreading around the system. Is that a fair characterization?

Jay Clayton:

I think that's a fair way to look at it.

Neel Kashkari:

Okay.

Jay Clayton:

I do. But I also think that the amount of capital that we have now backing up the financial system makes some of these exogenous shocks less impactful than they would've been in 2007, for example.

Neel Kashkari:

Yeah, fair enough. Fair enough. So we only have...

Jay Clayton:

I think two of your colleagues have got a good job of the core of the financial system. They're pretty darn resilient, which helps for these exogenous type risks.

Neel Kashkari:

Fair, fair. We have five or seven minutes left. Let me just shift a little bit. So one of your newer roles is that you're the non-executive chairman of Apollo, a very large private equity firm. You all have a lot of portfolio companies. I'm just curious in the... Where does cyber come up? Is this a regular topic of conversation with the portfolio companies that you're involved with? Does the private equity industry bring its own lens to cyber or is it pretty similar to the rest of the private sector?

Jay Clayton:

Well, I think that there's the... what I would say is the company itself, and then there are the portfolio companies. I can speak more to the company itself and then come back [inaudible 00:26:37].

Jay Clayton:

At executive committee, at the board of directors, cyber is a regular topic. It is in the deck. And going back to what I said at the beginning, I don't think the discussion is much different from it is at most places, which is it's a journey. We're all on this journey. We know we're going to have to upgrade continuously the reviewing our systems. We need human talent. It is an area where there is a shortage of human talent. We all know that. And you talk about those kinds of issues.

Jay Clayton:

What I will say is that I think that exposure to those portfolio companies, and not just in the area of cyber, but in other risk areas, it's actually beneficial because you have all the insight into all of these different types of industries and the risks they face, which range from financial institution type to media, to chemicals. All have cyber risks but are a little bit different. And that sort helps inform the discussion at what I would call the parent company, for lack of a better term.

Neel Kashkari:

Got it. Got it. And just a couple minutes left. As you look around, the world is changing. I mean, you mentioned that Ukrainian hacker for part of the group that hacked the SEC. Obviously, the United States relationship to Ukraine is very different than it was three or four years ago. Sometimes state actors are on our side and then the next day they might be on other sides.

Neel Kashkari:

Is there anything else happening geopolitically that jumps out at you as saying, "Boy, this is a new area that we need to be focused on"? I mean, when I think about cyber risk, I think about China, North Korea, Russia as the obvious actors, but are there other things that we all should be thinking about?

Jay Clayton:

Well, look, I don't like to be an alarmist.

Neel Kashkari:

Sure.

Jay Clayton:

But I think what we have seen in the last six months is that there are groups, countries, factions, whatever you want to call it, who benefit from destabilization. Some prices go up, some prices go down. Some people consolidate power, some people lose power and the like. A large cyber incident is a destabilizing incident. And so to think that nefarious actors aren't thinking, "Can I profit from this type of thing?" They're seeing that maybe they can. I think that we should be quite cognizant that that's in the toolbox of sophisticated world stage actors.

Neel Kashkari:

Yeah. And to your point, it's a nice reminder. The motivation might be profit, but it also might just be destabilization itself. And that's an end in of itself. Here, we run at our colleagues around the system, run economic scenarios of all sorts of different shocks that could hit the global economy. The nature of these shocks is they... Usually, the shock that hits you is not the one that you were looking for. It's kind of the tried and true.

Neel Kashkari:

So for example, all the different shocks that we've been looking at, we didn't have pandemic in 2020 is one of our top shocks. But of course the pandemic hit us and we do try to model, what if there were a big cyber event? And it's just so hard to know. Does it end up being a pretty contained event, in which case it's not a big deal for the US economy, the global economy, or that something much bigger, much more widespread? I think everybody struggles with this, and it goes back to where we started. How do you know if you're doing enough?

Neel Kashkari:

One of the things that I've learned over and over from our cyber experts is the vast majority of hacks and compromises are when institutions don't do the basics. You don't do the basics well and somebody's able to take advantage of that. It seems like it's much more rare that you have a highly sophisticated actor going through a very complex scheme to weed their way. And it does happen. Obviously, that does happen. But even if the banks that are watching this, that are participating in this conference, if they can just make sure that they are doing all of the basics well, it'll go a long way to making sure that they're protected against the vast majority of cyber risks.

Jay Clayton:

Yeah, I agree with everything you said. Your paradigmatic is the sophisticated state actor, but some of the risks come in the most rudimentary ways.

Neel Kashkari:

So when you look at the... Just to stay on the SEC for a moment in the last minute when we have left. When your team did after action review to understand what had happened so those hackers could get it through, was it highly sophisticated or was it basics of most blocking and tackling that many institutions come up short on?

Jay Clayton:

I think what I could say is it was a combination of both. The intrusion was the sort of type of basic failures. What they did with the intrusion was fairly sophisticated in order to not be detected and the like for some period of time. And I will say those exercises that you go through, even though they may not map to what actually happens, one thing in addition to communications that they reveal is authorities. And as a regulator, you're always wondering in a time of crisis, what authorities do I have, what don't I have? And just having familiarity with the tools that are available to you and your regulatory colleagues, I think is hugely valuable when you are faced for that unanticipated crisis.

Neel Kashkari:

Great. Well, Jay, I want to thank you. This has been a great conversation. I knew you'd have a rich set of experiences from which to draw. We really appreciate you taking the time with us, and I thank you for that. And with that, I'm going to turn it back over to our host. So good to see everybody. Thank you.

Matthew Tolbert:

President Kashkari, Jay, thank you so much for sharing your insights on cybersecurity risk and financial stability. And everyone this ends the YouTube broadcast of their discussion.

Matthew Tolbert:

Okay, everyone, we have now reached our second break of the day. We will be back at 1:45 PM Eastern Time for our...