Episode 3 – Building a More Resilient Banking System

SULTAN MEGHJI: Welcome back to the FDIC Podcast, a place where we talk about all kinds of things having to do with our banks and your money.

I'm Sultan Meghji, the FDIC's Chief Innovation Officer and today is very special for me. We're launching a new series of the FDIC Podcast that examines the particular issues related to technological innovation in banking.

In our first episode, FDIC Chairman Jelena McWilliams and I discussed the main themes we're moving full steam ahead on—that as we promote and encourage innovation… as we build the banking system of the future…we make sure that it's open and inclusive. And that it's resilient.

Today, we focus on resilience—how we protect our financial system from malicious threats so we can all sleep at night knowing our money safe and sound.

I am so excited to welcome a special guest to the FDIC Podcast, my friend and former Homeland Security Secretary Michael Chertoff. Secretary Chertoff has spent most of his life in public service – from being a former federal prosecutor who took on organized crime…to being a U.S. circuit court judge who later served on the U.S. Court of Appeals for the Third Circuit, and he was the second Secretary of the U.S. Department of Homeland Security.

Secretary Chertoff, thank you for joining us!

MICHAEL CHERTOFF: Great to be here.

SULTAN MEGHJI: So, let's just start off with something very basic. What does resilience mean to you?

MICHAEL CHERTOFF: Well, sometimes I tell people resilience is the ability to take a punch and get back up on your feet. But to be a little bit more specific, I think they're really three elements to what I consider resiliency. One is defense in depth, recognizing that when you're facing a threat or a risk, having a single point of defense is really putting all your eggs in one basket. You want to have multiple ways of defending yourself because you recognize that one level may fail and you want to have a backup level.

Along with that, I'd say resilience involves backup planning. What do you do if things go dark, if there is a glitch, if there is some damage to the system, how do you get back up again? That may involve having an alternative pathway, it may involve having an alternative set of records, and we could talk a little bit about that later, but it means not again, having all your supply chain be with a single point of failure.

And finally, what's your recovery plan? Once the immediate crisis passes, how do you return to the status before the event happened? All of those to my mind are what are resuming the word resilience.

SULTAN MEGHJI: When we talked about resilience in the banking system, a lot of our conversations are around software, and it's around process, and it's around people, right? And so, I hear everything you just said, and it's very easy to only think about it as a technology problem, but it's also a human problem, it's a process problem. As you've studied resilience and really shine...shone a light on this over the last few years, where are the first places that you've seen people be successful, approaching a discussion around resilience, that they haven't necessarily approached previously?

MICHAEL CHERTOFF: Well, I think, you know, when I first started out looking at cyber security issues and it was treated as a perimeter issue. Like a Maginot line…you've got to have a very strong set of gates to prevent people from coming in around the perimeter, and then we're done. That's actually almost the least significant thing.

An interesting way to look at it is the way we look at health and what we're going through now with the virus. If you went to your doctor and said, "Doctor, what can you give me, so, I'll never get sick?" He'd laugh you out of his office. Resilience in the healthcare area means the ability to lose some infections, but also to be able to recover quickly, to be able to have palliative care that allows you to function, even if you are somewhat ill, the ability to intervene if necessary, even to remove something that's dangerous. That's what we've begun to move to with the internet. We're looking now at layered defenses. How do we, for example, segment the network so that once you're in, if I can use the analogy, the infection doesn't go all over the place? How do you use identity to manage who gets to do what and who has power to do something? How do you have an alternative set of records, if your records somehow become inaccessible? All of these are now elements in what I consider to be a strategy of defense and resilience, which increasingly we are migrating toward.

SULTAN MEGHJI: This almost sounds like you're talking about an immune system.

MICHAEL CHERTOFF: It is. And as you know, with your health, it's not always the case that when you get a single vaccination or a single pill you're done for life, you have to keep boosting it. And you also have to have the ability, in the case that something in fact does get through the immunity, to be able to reduce the effect and to recover.

SULTAN MEGHJI: Well, I mean, this is exactly what we're dealing with, with the COVID vaccines, right? I mean, you know, the current generation of them don't make it impossible for you to get it, but it allows you to mitigate the effects of it, you know? And at some point here in the future, there

will be full immunizations, one would assume, that would then make it harder to get in. But getting back...

MICHAEL CHERTOFF: Yeah, let me say that that's exactly right. And one of the key lessons in both cases, cyber-attacks and health, is that you need to understand risk. Risk is not a zero sum proposition, I want no risk ever. Even if you stayed home and never left your bedroom, there'd be some risk that your roof could fall in. What you have to do is reduce the risk to a level that is tolerable and then have ways to mitigate the effects. So, that again, you can be resilient and that's really the key to resilience.

SULTAN MEGHJI: It's so interesting to hear you talk about no longer thinking about the Maginot line, you know, because, you know, we're just at this moment where we're starting to talk about zero trust networks, which is, you know, kind of the logical next step… to go from the moat version of perimeter defense, with VPNs and things like that, that we've had for 15 years, to now think about entire environments that are zero trust environments, right? And as we go into this next stage, so many banks, and so, let's try to make this real for so many of our listeners, you know, so many banks are using really old technology, right? These are decades old systems in some cases, and they're using more modern fintechs to expose some of what they do. As you're taking the very old and combining it with the very new, the opportunity for risk is not zero, obviously.

MICHAEL CHERTOFF: Correct.

SULTAN MEGHJI: And so, one of the things that I think a lot of our banks struggle with is figuring out how to take the discussion of risk, that you and I are just having here, and making it real in terms of how they think about initial next steps. You've got a tremendous visibility across, not just this market, but other markets, are there some things that you're noticing that people are doing that are good first steps to try to approach resilience at an almost an organizational level?

MICHAEL CHERTOFF: Well, one thing we're hanging...we're advising clients on is to look at your business model, look at what your key assets are and look at who the threat actors are. Because not every entity is subject to the same threats, and then tailor your emphasis on defense to those threats that are the most serious in consequence, and most likely to happen. And that could be in the case of a bank, it could be obviously theft of money and a theft of other valuable assets. But it can also be, for example, interfering with the availability of the banking system by shutting it down.

Some years back, I think in Britain, not because of an attack, because a mess up with a software, one of the banks went offline for a while and that becomes very, very debilitating. You also want to look at the integrity of the data. More than many businesses in many industries, banking is about information. A nuclear power plant either has its powers on or it's off, whether the radiation is spilling out or it's not. But banking only works if there's information that is accessible and reliable. And so, again, the danger of corruption of data, or ransomware which shuts down access to data, is very, very salient to the banking industry. So backup plans, alternative sets of records, alternative ways of recording transactions are some of the steps bankers can be thinking about as kind of initial giant steps to security.

SULTAN MEGHJI: You know, we have about 5,000 banks in this country, right? Of a variety of different scales, of a variety of different technical capabilities and probably 20,000 different supporting organizations, whether it's FinTechs or other technology vendors. And so, looking at that landscape, even though we don't directly regulate a big percentage of that, we wanted to to shine a light on this and begin to help this community figure out how to address these kinds of issues. We've talked about threat landscape a little bit, but as you think about, putting yourself in the shoes of a banker for a few minutes, what are some of the threats? What are some of the things that are top of mind for you?

MICHAEL CHERTOFF: Well, we've seen of course, the theft of money. And, you know, as Willie Sutton said, "I rob banks because that's where the money is"…but what has happened with cyber-attacks is the scale of the robbery has been much greater and nation states who've been involved. So, in North Korea, for example, for a long time has run a series of efforts to basically withdraw millions and millions of dollars from ATM's by corrupting the systems inside the ATMs or the cards and thereby allowing limitless withdrawal.

So, figuring out whether there's a vulnerability there and how you might mitigate it…maybe it's dual authentication, maybe it's lower withdrawal limits, maybe it's some kind of a behavioral analytic that tells there's an odd pattern of withdrawals. But that issue of withdrawing a lot of money is one element.

Another thing the North Koreans did was use bank transfers, interbank transfers, as a way of stealing money. So, you know, a couple of years ago, the Federal Reserve Bank of New York received instructions from the Bank of Bangladesh to send over a billion dollars to overseas banks. And about 80 million were sent before somebody noticed some oddities in the language of the instructions and said, "Timeout, this looks funny," and they called a halt. But again, because the banking system is global and the need to move money efficiently is a very high priority, that again is an issue, you've got to think about.

Availability…I'll give you another example…we did an exercise, I did with a bank board of directors a couple of years ago and this is where planning becomes important. And the scenario was that the vendor for the bank cards has been corrupted by a cyber-attack. And we now don't know if the banking cards and the credentials are actually real. What do we do? Do we shut down until we can verify things? Or is there an alternative? So, as we worked through it, I said, "Look, you must have some clients that have a regular pattern of withdrawal and transactions every week or every month, like payroll. On those you probably don't need to work very hard to verify identity because you've got an existing pattern of behavior that validates as long as it continues. But if there's a singular transaction, that may be where you're wanting to say, "Time out, we've got to look at this." So, this was not a technology solution, it was looking at behavioral data that you've collected and analyzing how that can be used to mitigate the risk.

SULTAN MEGHJI: Well, this is a great area of focus because there's a lot of discussions in the banking sector right now about artificial intelligence. And, you know, there's been some House hearings here recently, and there's going to be more of that. And there's this notion that artificial intelligence, is an entire category and that we need to think about AI and any sort of algorithmic

automation as one single bucket. And I would encourage people to take a more nuanced approach and say, "What are you actually doing with it?" Right? You know, AI, that's used to make credit decisions, for example, is one thing, and using AI, as you've just described, which we already use in market for things like Bank Secrecy Act, and anti-money laundering, and other fraudulent activities is becoming fairly commonplace very quickly, right?

There are a lot of organizations out there that still do all of this by hand. They have people sitting at computers and they see a transaction pop-up and they say, "Okay, I'm going to research that for 20 minutes and decide if this is kosher or not. I would be very curious to hear what you think about in working with bank boards, for example, how you get these organizations and the people to kind of step up and say, "Yeah, this is something we need to be putting front and center."

MICHAEL CHERTOFF: Well, I think, you know, a lot of the challenge you have with boards, not just banks, but with all kinds of companies, is they have so many problems and solutions that are being thrown at them, that they become overwhelmed and they feel like we get bankrupt ourselves just by bringing you all of this online. So, how do we decide what's worth doing? And that's why I go back to risk management. If you can explain to a board, here is where your highest risks are, both in terms of threat and consequence, and then you can give them not perfect solutions, but things that can really reduce the risk in an efficient way. You know, I have found that boards gravitate to that.

Now, sometimes it may also involve making a decision not to get involved in a certain kind of business or certain kinds of transactions and banks already are dealing with a need, for example, for artificial intelligence in 'know your customer.' So the key is how do you adapt machine learning, artificial intelligence on the security side and in terms of risk in general, but also recognizing it, the final decision in many cases should be by a person. But what the artificial intelligence can do is reduce the surface area in which you're having to make decisions and tee it up for a quicker answer.

SULTAN MEGHJI: How do we get more people to think about resilience, to think about making it part of their career, to think about making it part of their daily lives, not just at the board, but at the consumer level?

MICHAEL CHERTOFF: Yeah, well, I think a lot of this is at the consumer level. We need to get people to understand the value of things that are resilient and security focused. But we also need to make it, we need to demystify it because to be honest, I've dealt with, you know, a fair number of engineers who feel more complicated they can be the more authority they have. And what it really does is it causes people to withdraw.

One of the great examples of an area that we need to do work, is passwords. Passwords are inherently limited in utility. The more of them you proliferate, the harder is to keep them straight, if you have to keep changing, and that becomes difficult. Now we're beginning to move more to facial recognition. If, for example, a multifactor authentication with facial recognition, maybe analytics about the device you're using, as well as some vision of your normal behavior…if those were brought together, it would both make it a lot easier for the consumer, but it might also be even more robust.

SULTAN MEGHJI: Absolutely. Well, I mean, one that we hear commonly added to that list is geolocation. So if my car and my phone are not within walking distance of each other and my phone starts doing something extraordinary, from a banking perspective, maybe it shouldn't be allowed to do that. Right?

So, on the human side, it would be impossible to talk about resilience without talking about where we want to go with it. You and I have just been having a very nice conversation that I hope people found interesting about kind of where we are and how we got here. Decades of technical debt, decades of this. I take a step back and think about this at almost a macroeconomic level. We're in a huge moment of evolution in the banking sector and in our nation's history. We look at other nation states challenging us from a foreign policy perspective, from an economic perspective, we see independent financial structures, like some of the digital assets activity emerging. And then there's a tremendous amount of discussion we could have around that, probably better for a different time. But then we also have to think about where we as a nation want to go. And as someone who's been a public servant for a huge amount of his career, one of the questions that I came into this really wanting to hear you speak about was how do we create a 21st century where the United States is still the number one, where it's still the leader, where our competitiveness is second to none in a way of kind of looking at what we did in the 20th century and doing it in the 21st century? So how do we, how do we do that?

MICHAEL CHERTOFF: Well, I mean, one of the keys to our leadership role in the last, you know, decades was the financial sector. And the fact that we were…the dollar currency was the backbone of global finance. That's why the Chinese have worked very hard, and not particularly quietly, to try to create an alternative financial system and alternative financial vision because they feel that as long as we are the dominant financial force, we have leverage. And I think that's going to continue. And that will also involve convincing people that the stability of Chinese currencies is tantamount to the same as the US…as well with issues about trade and where we use tariffs, and where we don't use tariffs. And of course the supply chain and whether we are wholly reliant on China.

One thing that we've seen about China in the last few years, since Xi became president…because that really was an inflection point…is the use of economic power for geopolitical ends. You know, for a long time, the U.S. took a very purist view. Commerce is commerce. Businesses is business. It pursues the profit motive and we don't tell it what to do. You know, our geopolitical strength is the military, our industrial base, et cetera. That's not the view of the Chinese or the Russians and they will use their economic power as a way of not only taking intellectual property, but really basically saying to other countries, you do this or we're going to pull the plug.

At the same time we've begun to do a little bit of that too with sanctions. And one of the key sanctions tools we've used against the Russians has been to cut off certain people from the financial system. Now we haven't totally cut Russia off, but that raises a risk too because it makes the financial system part of a battlefield. And at some point, you know, there's a concern that if you overdo it, the Russians might say, "Well, what the heck? We're going to just, you know, interfere with the ability of system to operate." So, as with most things, there's a technical element to how we protect our position in the financial system as a world but there's also a human and strategic element. We want to acknowledge that we have to use sanctions sometimes but we don't want to overuse it to the

point that we wind up actually getting blow back. And I think these are going to be big challenges for the next few years.

SULTAN MEGHJI: Yeah. It's interesting to hear you talk about, and I do hear a comparison between belt and road, which is the PRC's mechanism by which they use capital to in essence buy cooperation especially in Africa and other parts of Asia with our sanctions environment. And if you look back to, for example, the 1960s and 70s, with organizations like USAID and kind of post-Marshall Plan activities, we really did finance a lot of the development of the world. Not just the rebuild after World War II, but that kind of big industrial boom in the mid-20th century. And then we followed that on with the internet, boom. These were kind of sequential activities, right? I look to the next 50 years and say, "You know, sanctions is one thing that we have to be calibrated very carefully on," because, you know, the last thing I think we want is total economic warfare, that's not good for anybody. But then figuring out what other things we should be doing. And, you know I joke in speeches that at some point Elon Musk is going to put a bank on Mars. And so how does that work? How do we make sure that's part of the American banking system and not part of the PRC's banking system?

MICHAEL CHERTOFF: Well, that's a great question. I think that, you know, there are a number of different dimensions to it. One, is of course, just facilitating American investment in the Southern Hemisphere. We're starting to do that a little bit more in Asia and in Africa and if we can present people in those parts of the world with an alternative way to run technology, in which they don't feel that we're, you know, we're going to steal their technology or their intellectual property or otherwise use it to leverage them, we will then attract those customers to American enterprises or Western enterprises and not to Chinese. By the way, this should be collaborative with Europe and other like-minded nations, it's not really just America.

SULTAN MEGHJI: Well, I think it's worth saying that a number of people now are talking about this kind of D-10. Where it's the kind of 10 largest democracies are kind of aligned. I think it would be wonderful if we could all kind of get behind each other, not just in terms of being democracies but also being free market capitalist economies.

MICHAEL CHERTOFF: Well, I'm a big believer in that. And we're trying to do this now by building, for example, coalitions to do investment in critical infrastructure technology like chips, like 5G, where we don't want to simply have Huawei be the default company that does the 5G infrastructure but we want to work with our European allies and other democracies to have other companies be able to come forward and be competitive. And that means we don't then give the Chinese the leverage that being a sole source has.

And one thing that pandemic taught us, was that the mentality a lot of businesses had for a long time which was described as…lean, just-in-time, don't have anything you don't need in in the next 10 minutes…turns out to be a great way not to be resilient. And for example, the auto business now is having a problem because they didn't have any kind of a backup plan with chips. So, when chips dried up from China, all of a sudden, they were like, "what do we do now? We have to shut down."

So, I think part of this mentality of resilience, of investing in parts of the world where we want to build good relationships, those are positive ways of counteracting geopolitical rivalry as opposed to just punitive things which are sanctions.

SULTAN MEGHJI: Well, it' difficult for us, I think, to not take a very hard look and see autocratic, highly centralized, political economic systems which is basically the definition of socialist and communist platforms, right? And then compare it to ours, which is much more federated. And I'd much rather have 15 manufacturing sites for something scattered across three continents than one in one place. It's an absolutely fascinating problem and I think if I was sitting in a job like this as a regulator in Brazil or Australia or India, I would see two very different, characteristically different, systems. I'd see a highly regulated, highly controlled, highly centralized PRC system backed by the CCP and this kind of wild, wild West almost on the other side. And I think there's an opportunity for us to draw a better picture or draw a better comparison and in doing so, create more market opportunity for the banks of the United States, which to me gets exciting.

MICHAEL CHERTOFF: I agree, and I think the key is not to duplicate an autocratic system, but it's also to recognize we have to be strategic…that simply saying everybody do your own thing doesn't really work when you're dealing with a hyper-competitive global environment. And so I think we can be strategic without being coercive or over-regulating.

SULTAN MEGHJI: You really understand this better than a lot of other people. So, first off, thank you for coming today, this has been great…but what brings that optimism? For those who aren't in the room with us, you know, the Secretary has been sitting here kind of smiling the entire time and maybe we'll get some pictures or something, but there's a clear optimism in your voice. What brings you that optimism?

MICHAEL CHERTOFF: Well, you know, first of all, the fact that we're doing this, the fact that you have resilience focus now at the FDIC and I'm seeing this in other parts of the government as well, and I'm seeing it overseas. I think we've now woken up to the fact that we need to really take a look more holistically at how we run our economy, how we run our activities in cyberspace and where we are geopolitically. And once we start to look at it strategically, we will come up with solutions. They won't be perfect, but we won't be simply conceding the battlefield by default. So, that gives me cause for optimism.

I also think generally when it comes to ingenuity and technology, the West still has a tremendous leg up over other parts of the world in terms of creativity, in terms of energy. But the one thing I would say to come back to the point you made a moment ago is this, I worry about overregulation too. So, one of the things when I was at Homeland Security that we used to say is this, "We want to be outcome-based…we want to tell the companies that we regulate or we have some say over, here's what you have to be able to do. Exactly how you do it is up to you and it can fit within your structure, in your plan. And we're willing to help you and give you advice, but we're not going to micromanage you." And that to me, is the right balance. If you tell people here's what you have to do and the capabilities you have to have…and most important…if you tell them you need to have a plan and we need to be able to see the plan, then you give them the ability to figure out within their particular context what is the most efficient way and the most cost-effective way. As long as we take that

approach, I'm confident we can catch up on some lost ground. And I don't want to make the Chinese or Russians larger than life. They have big problems of their own too. But the key thing is here, we finally have noticed we need to get moving and that's good that we're doing it through plans, like what you're describing.

SULTAN MEGHJI: Fantastic. Well, thank you, Mr. Secretary for joining us today, it's been a pleasure to actually sit in the same room as you for the first time in a year and a half…yeah, it's been awhile. So thank you, sir.

MICHAEL CHERTOFF: Thank you. And good luck.