FDIC
PODCAST
SPECIAL SERIES
Banking on Innovation

Episode 4 – Protecting the Banking System

SULTAN MEGHJI: Welcome to the FDIC Podcast, special series *Banking on Innovation*. My name is Sulton Meghji, the Chief Innovation Officer here and with me today, I'm just so excited to have my friend Tim Maurer who I met millions of years ago at Carnegie and now has one of the coolest jobs I think in the U S government. So first off, Tim, thank you for doing this today. It's great to see you again.

TIM MAURER: Thank you so much for having me. It's great to be here.

SULTAN MEGHJI: Fantastic. So for our audience, why don't you tell everyone what your current job is?

TIM MAURER: Sure. So in February I joined the Biden-Harris Administration as the Senior Counselor for Cybersecurity and Emerging Technology to the Secretary of Homeland Security, Alejandro Mayorkas. So, I'm his principal advisor in his office on all things cybersecurity and emerging technology. And as you can imagine, it's been a fairly busy the past few months, since I've joined.

SULTAN MEGHJI: That is, I believe, one of the biggest understatements I've ever heard to say it's fairly busy, even in our world in banking...that is those two topics between cybersecurity and emerging technologies dominate so much of what we do here at FDIC and certainly in my role. But for people who don't know you, I mean, I have the luxury of having known you for a while, but for those who don't know you, what's your story? Like what got you to February of this year?

TIM MAURER: So as you know, prior to joining the administration, spent the past years working at various think tanks in Washington, DC, focusing on cybersecurity policy and emerging technology. I joined the transition team that prepared for the new administration and was focused on what should be the various policies and first actions that we should take with respect to cybersecurity in the first several weeks of the administration. So in September I joined the transition team and it was working with that, a small group of people that built on the work that was done during the campaign and essentially thought through what do we need to do day one, the first week, the first couple of weeks. And as you will recall, the Solar Winds incident in December, just further drew attention to the importance of cybersecurity and how much work there remains to be done.

SULTAN MEGHJI: As we go through, you know, this journey from, the think tank world to the transition team. And then now as this advisor to the current Homeland Security secretary, I look at a variety of different actions that, that we've been trying to do at the federal level. You know, there has been an executive order around zero trust, a couple of other things like that...as someone who's also newer to government, how has that transformation gone in terms of taking, you know, things we know are big priorities and actually turning it into action. What's that been like just from a human process perspective, like learning this?

TIM MAURER: It's a great question. I think, you know, the first time I was confronted with how to navigate that was when the secretary gave his speech on March 31st outlining his vision and in the weeks prior to that, and leading up to that, the question was how do we provide a sense of order and a roadmap, given that the Department of Homeland Security is responsible for critical infrastructure protection across various sectors. He, as the secretary, is not just the secretary for cybersecurity, but obviously immigration and a lot of other things that the department is focused on. So the way we were able to navigate that was we essentially drafted this speech that provided a vision for what the department would focus on, but then operationalized it through this idea of 60-day sprints, where we would identify specific priorities and then channel the Office of the Secretary and drive action across the department, but also working with our partners through this idea of having dedicated 60-day sprints in addition to the more medium- to long-term priorities.

SULTAN MEGHJI: Was that a big cultural shift for the organization? Was that like, did, did you have to spend a lot of. Blaming what a sprint was and what a scrum master was and things like that?

TIM MAURER: So, I think some people are, I remembered a sprint that took place a couple of years ago across the federal government to just drive a certain cybersecurity measures. But the way we designed it across various components of DHS and having them consecutively focused on different issues, I think that was new to the department. But the idea caught on very quickly. We have a fantastic policy team and a fantastic cyber team that we worked with very closely to put together an action plan for the sprints and to then execute and drive action. So I think people felt excited about it. It provided a clear kind of roadmap and vision. And you know, in between, we had the occasional cyber incident that we had to obviously manage and then also take them into account as we thought about policy development and next steps for our work.

SULTAN MEGHJI: You know, for those who didn't hear the Secretary speech on March 31st, would you mind giving a couple of high points that you think would be worthwhile for the audience to hear?

TIM MAURER: Yeah, of course. So what the Secretary outlined in his speech was that cybersecurity is a top priority for this administration. Following the Solar Winds incident where we had this massive campaign exploiting Solar Winds and then infecting several thousand Solar Winds customers. The President-Elect at the time already issued a statement making clear that cybersecurity would be a top priority. It is one of the top priorities for the Secretary himself. So what the speech outlined was, one, that this will have his attention throughout his tenure. Two, that too often cybersecurity is thought of as a stand-alone value, but that we need to recognize that cybersecurity is something that we need to think through with respect to our values and principles and how we just think about how we go about security generally as a society. And this will, I think, also with respect to the ongoing discussions about artificial intelligence, there are some, some important analogies here. And then he outlined the series of six sprints. The first one was focused on tackling ransomware more effectively. So this was in March…pre-Colonial…because we were, at the time, very concerned about ransomware attacks, specifically targeting hospitals and healthcare facilities. And specifically with respect to the rollout of the vaccine, we were worried that ransomware attacks posed a risk that were at the level of a national security risk, that we needed to elevate in terms of a priority for the department and for the country to focus on.

The second one was focused on the workforce and actually led to the biggest cybersecurity hiring effort in the department's history where we brought several hundred people on board because we have this as a priority, I need to make sure we have the people to actually execute. And we are currently in the midst of the third sprint, which focuses on industrial control systems. So the kind of systems that run critical infrastructure specifically. And the next three sprints are going to focus on the transportation system, then the election infrastructure, and then last, the international dimension of our work.

And meanwhile, we have several ongoing priorities that we are very focused on, which is protecting the federal government in the wake of the Solar Winds incident and making sure that we put all of government in a better position. Second, making sure that we strengthen the integrity of the supply chain, which again, not just a Solar Winds, but also the Kaseya ransomware attack, highlighted the importance of making sure we think through the full chain of what needs to be secured. And then, protecting our democratic institutions and elections…you know, elections are always on the horizon.

And then last is focusing on issues that are on the horizon. So emerging technology. Where we can just be always stuck in the here and now, but we need to make sure we also keep a focus on issues that will happen in a couple of years and where we need to take a preparatory action now so that we are well positioned.

SULTAN MEGHJI: Yeah Tim, that's a great summary. And it just strikes me that I didn't hear two things in that discussion. I'm really curious where they land in this universe. So the first is, you know, we're a financial regulator, right? So, do you just trust us that we're doing such a great job that you don't need to make that a sprint?

TIM MAURER: That's a great question. When the White House released the national security memorandum in July that focused on critical infrastructure, the White House highlighted that the current approach is focused on individual sectors and that we have certain regulators that have taken actio n with respect to cybersecurity for specific sectors. But that is not across the board. And it also vari es significantly from regulator-to-regulator and how much cybersecurity has been something that they've focused on.

I think with respect to the financial sector, given that the fin ancial sector has been a target of malicious hackers since the advent of the internet, at least since it was commercialized i n the early in the early 1990s. I think the first major bank when New York Times article about a $10 million a heist was in 1994. The financial sector has been, in many ways, at the forefront for a lot of other sectors and has some very interesting lessons learned partly because a lot of financial institutions have enough resources to actually protect themselves against it.

But I would say that there also still remains work to be done in the financial sector to your earlier point about interconnectedness as sometimes the firm-level attention blinds the focus on potential systemic risks or the kind of nodes in the network where if the y are affected, could have a systemic impact. So I think there's been a lot of very interesting thinking in the financial sector that has been helpful to us. As we also think about other sectors.

SULTAN MEGHJI: Well, it's interesting. So one of the things we've done recently is started organizing vertical risk based on any institution or any subset of institutions versus horizontal risk, which is systemic because, you know, obviously the FDIC has this deposit insurance fund that covers a tremendous percentage of the banks in the United States. And one of the things that, that we are dealing with is that any one moment there are multiple, in fact tens in some cases, ransomware attacks against yeah. And that, that doesn't just have impact to those individual institutions, there's a network effect, there's a broader set of horizontal risk we have to consider. And that's something I think 10 years ago, none of us were really thinking about, or even 15 years ago. And so now this is a bigger part of our discussi on.

TIM MAURER: Yeah. And, if I may, the point you just made is actually really interesting because when the Colonial pipeline ransomware attack happened which occurred on a Friday. And we started tracking this in the front office Friday afternoon. And it was fascinating to watch how quickly the discussion turned from the immediate impact of the malicious cyber activity to the public's reaction. And here's a clear analogy to the financial sector, at least that's how I thought about it at the time, which was…we need to be very careful about how the public is reacting and the communications we are putting out, because this could quickly get into a point where we may have to worry about a run on gas stations. If people start being worried, not having access to gas and fuel, and that the public's reaction may aggravate the actual impact of the incident. So very similar to a run on the bank, you know, and then a few weeks later, TSA, which is part of the Department of Homeland Security, issued a first security directive for cybersecurity and the most critical pipeline owners and operators and required incident to be reported to the *Cybersecurity and Infrastructure Security Agency* at DHS, CISA as we call it…and the timeline for the reporting was set at 12 hours. And the reason it is set at 12 hours was because there was a recognition following the Colonial incident that public reaction piece of it is critically important and that for us as the government to know early on if there is an incident that could rise to that level of it being in the media…because once you shut down a pipeline, others are going to notice that you've shut down the pipeline…to be ahead of the curve when it comes to the public communications piece so that you can early on address any concerns and mitigate the risk of a potential reaction that makes the crisis worse than it could than it actually is. So it was a clear analogy here to I think some of the lessons learned from the financial sector.

SULTAN MEGHJI: Let's start talking about the future a little bit, because you know, one of the conversations that, for the audience that Tim and I've had a couple of times, is things that are coming. You know, whether it's some of the great power discussions that have started, whether it's quantum computers, where it's artificial intelligence, Tim let's start off with AI. Like what's, what's going on DHS…what's going on in your head…as it relates to artificial intelligence?

TIM MAURER: Yeah, it's actually quite exciting. When I joined DHS in February and got up to speed of what some of the work that had happened internally, DHS actually issued a dedicated strategy focused on artificial intelligence in December, shortly after the White House had issued its executive order focusing on AI…which outlined a set of principles for how we should be thinking about use cases and the implementation of machine learning and artificial intelligence to ensure that it takes into account some of the recent concerns around discrimination and make sure that we are thoughtful and careful about how we adopt new technologies.

So the DHS strategy has taken a lot of that on board and we are now in the process of thinking through how to implement machine learning and artificial intelligence across the various components. Whereas DHS, as I mentioned, you know, we have TSA, or we have CISA…there's Customs and Border Protection (CBP)…ICE, HSI, the Coast Guard is part of DHS…so there's a lot to think through in terms of what are the actual use cases of machine learning across the department. But we recognize that the country, I think, is coming to terms with how quickly the technology is evolving…is coming to terms with some of the challenging and some of the difficult ethical questions the implementation of the new technology is posing. But we are very determined at the DHS to be thoughtful and to be working, not just internally with our respective stakeholders, but also to be working with our external stakeholders and the respective privacy groups, civil liberty groups, industry stakeholders to discuss with them how we can do this in a thoughtful manner. And, as you know, continue to be discussions about how to implement certain technologies like facial recognition or others in a thoughtful way. So, it's top of mind for us and we're excited that we were one of the first departments to have a dedicated strategy focused on AI and to continue to implement it.

SULTAN MEGHJI: You know, beyond artificial intelligence, I worry personally five or 10 years out. I worry about issues with our workforce. I worry about this interconnectedness. I worry about debt, you know, technical debt in the system…you know, old computers, old networks. We see a path with zero trust architectures…we see a path with kind of self-healing systems and some of the more interesting things people are doing with artificial intelligence…that kind of an infrastructure layer. But there's a lot to do between now and then. And, you know, having a policy is great. Having a strategy is great, but you know, we're seeing a fundamental shift in the workforce. We're seeing a fundamental shift in how we implement technologies like this. And, you know, the federal government is never really ever the first to do anything. And, that's my understatement of the day! DHS is at this nexus of so many different things going on, you know, can you, can you share a little inside baseball with us about how you guys are thinking about how to position us as a nation for 10 years out, 15 years out?

TIM MAURER: Yeah, I think that's, that's the big question that everybody's asking How do we train and find the right people, but how can we actually do it at scale considering this broader tech revolution that I think we are all going through.

What we've done at DHS at this point…and you know we're five months into the new administration, but there's been a lot of work that has been done in prior administrations as well. Within the department, first, have the second sprint dedicated to the workforce, to bring people on board and fulfill empty billets within the department and just make sure that we have the people to execute our mission. And that continues to be something we will remain very focused on because, as you know in our field, people may switch and join industry a few years down the road. So, you can't just assume people will stay with you for five or 10 years, but you have to constantly make sure that you draw attention to opportunities, that you recruit people and that you train people who internally may want to follow that path and may have been in a different trajectory before.

What we've also done…the speech that the Secretary gave on March 31st was actually an event that we deliberately partnered with the Girl Scouts of the USA and with Hampton University, which is a historically black university that is a recognized center for cyber excellence by both DHS and NSA. And we also partnered with RSA. And the reason we wanted to partner with these various stakeholders is one, because we are the department of partnerships and to reflect that in terms of the actual event, but we specifically wanted to partner with the Girl Scouts of the USA because we wanted to highlight that it's important for us to already be thinking about that pipeline. And how do we inspire the next generation of people to pursue a career in cyber, to pursue a career in stem…starting in high school and then ideally in college?

SULTAN MEGHJI: It's absolutely fantastic. And, and, you know, I think I say this all the time, but it's good to hear someone else say it, which is, I don't think a lot of people recognize just how much technology is changing in some of these sectors in such short amounts of time. You know, I think it's taken as given now that, that we've had more technology change in the financial sector in the last two years than in the last two decades. And, you know, I don't think people get that and understand that there's great opportunity with that, but there's also risk with that and that in the face of us being the most targe ted nation, we have the most attacks against us of anywhere in the world. And some of its criminals, some of its guys in basements, and some of it is nation states and, and that they all have characteristically different views to them. And so, you know, there's the old line about offense. Offense only has to be right once. Defense has to be right all the time. And his is a core thing that's now part of everyone's lives. You know, when we talked to bankers, I always say, if cyber isn't one of the top two or three things you're thinking about, I would ask you to consider what your top two or three things are.

So Tim, with that, you know, I just, I have to thank you so much for coming and participating in this. This has been hugely interesting, and I'm glad that the audience got to hear some of the thoughtfulness and activities you have going on. I'm going to end with two questions. Okay? So question number one. In your role with what you're seeing today, with everything that's going on, what would you want the financial sector to hear from someone like you?

TIM MAURER: We are at a pivotal moment in time when it comes to cybersecurity for the nation. If we look at the past several months and the various cyber attacks we've seen, they have highlighted that the threat is proliferating and becoming more serious in terms of the impact it's having. But it's also highlighted some of the vulnerabilities that we still face.

So with respect to the financial sector and leaders in the financial sector, it's critically important to think about how can we improve the defenses on the front end to avoid being hit by a ransomware attack or other malicious activity. But what we've also experienced is that we cannot assume that there will be a 100% security and that we need to have a plan in place if something bad does happen and to include the public communications piece and to include how to work with government and to sh are information with government so that that's in place early on.

I will also say, looking back eight months ago and you would ask people on the street if they had heard of Solar Winds or Kaseya, I guarantee you most people had not. And what those incidents, I think, have also demonstrated is how, to your earlier point, how much technology has been changing, how much of that technology is actually being driven by some companies that pe ople have never heard of before and that if you work in a financial institution, it's important to fully understand all of the technology you are using and what your potential vulnerabilities are with respect to your supply chain so that you can, on the one hand, improve your defenses, but also make sure that you're resilient across the full spectrum of if there are certain failures were to occur.

SULTAN MEGHJI: Well, you've said one of my favorite words, which is ‘resilience.’ And that gets to my second question. So thank you for teeing that up for me. Recently we had former Homeland Security Secretary Michael Chertoff on, and we spent the entire time talking about resilience, which is, you know, a super set around, around cybersecurity. And one of the biggest challenges I think for so many people in the sector is they think about cyber and they think about tech or, and or they think about resilience and they think about tech and, you know, so many of the key vectors of attack for those people are not strictly a technology attack…it's a human attack or it's a backhoe or it's a flood or a tornado. You know, there are all these things that hit at our resilience. We've spent most of this time talking just about one of them, which turns me to my future question for you over the next few decades…What do you think are going to be some of the biggest impacts to the resilience of our nation, especially as it relates to critical infrastructure. And I obviously care more, you know financial services, but answer the question more broadly. If you feel like it.

TIM MAURER: I would answer that with two points. The first one is the nexus between cyber incidents and non-cyber incidents where a lot of institutions have already very mature, well-exercised plans for a natural disaster. They now have plans for pandemics because of COVID-19. What we experienced in the wake of the Colonial pipeline, that ransomware attack, was it started out as an it cyber incident but within two or three days, it quickly had spiraled into concerns around a disruption of the supply of fu el, gas more broadly, where at DHS with, the Jones Act and FEMA, we quickly transitioned from a term from a cyber response to a broader DHS-wide response. And that connection when a cyber incident morphs into something broader is something that financial institutions face as well. And making s ure that you don't have separate plans just for cyber incident and for non-cyber incident, but that you also think about how some of those may could come together and what the transition points I think is very important.

The second point I would make is we already know that some of the emerging technology is likely going to have systemic impact or is going to revolutionize certain parts of the way we do business or the way we operate. The impact of machine learning, some of the discussions around the potential impact of quantum computing on things like encryption algorithms and the need to transition to post quantum encryption algorithms, NIST at the department of commerce already has a process underway.

So those are some of those issues where, in order to be resilient against those technological breakthrough moments, it's important for organizations to think about those early on and to develop a plan so that they can buy themselves time, given that the pace of technological innovation has tended to outpace at least the government's ability to react quickly.

SULTAN MEGHJI: I don't think anyone's going to be shocked to hear me say that, that there are a couple of sectors that always lag on keeping up with technology and then the government has historically been one of them, but also the banking sector has also historically been one of them so it's not just that we're, we have a lot of these active and future changes, but that they also are kind of having to speed up anyway, because you know, they've been working on technology from 10, 15, 20 years in the past.

Well, with that, Tim, I know you're incredibly busy, but I just wanted to thank you again for coming and participating in our podcast. This has been hugely interesting, and it's always great to have a good conversation with you. So thank you for so much for joining us today.

TIM MAURER: Thank you so much for having me. Thank you very much.