Teneo Insights Webinar: Risk Radar

Teneo Insights / May 13, 2021

Alexandra Lager (AL): Good day and thank you for joining today's Teneo Insights webinar. A recording and podcast of this call will be available on Teneo's website. And now I would like to hand it over to our host, Kevin Kajiwara.

Kevin Kajiwara (KK): Thank you Alex, and good day everyone. And thank you for joining today's edition of Teneo Insights. I'm Kevin Kajiwara, Co-President of Teneo Political Risk Advisory in New York City. Well, if we needed any reminder of how vulnerable the nation's companies and our critical infrastructure are, the DarkSide ransomware attack that resulted in the Colonial Pipeline shutdown over the last several days, and which has seen spiking gasoline prices in the Eastern and Southern U.S., has teed up today's call perfectly quite frankly. And yeah, we're here to talk about not only cybersecurity but crisis preparedness and threat intelligence and response planning and management. And we're very fortunate to be joined today by actually perfect timing here as well, Teneo's two

Juliette Kayyem
Senior Advisor
juliette.kayyem@teneo.com

Rhea Siers
Senior Advisor
rhea.siers@teneo.com

Kevin Kajiwara
Co-President,
Political Risk Advisory
kevin.kajiwara@teneo.com

newest senior advisors are with me, and I can think of nobody better positioned to talk about these issues. So, let me introduce them now.

Rhea Siers. She has over 30 years of experience in the U.S. intelligence community. Among other things Rhea served as the National Security Agency's Deputy Associate Director for Policy, and she was their Senior Representative to the FBI. She also served on the Executive Committee of the Joint Terrorism Task Forces in New York, Washington DC and Miami. She is the co-author of Cyberwarfare: Understanding the Law, Politics and Technology, among other titles. Today she's on the faculties of Johns Hopkins, George Washington University and American University, and most recently served as Cyber Defense Strategy Executive at Bank of America, focusing on cybercrime and threat intelligence.

Juliette Kayyem served in the Obama administration as the Assistant Secretary of the Department of Homeland Security for Intergovernmental Affairs. Previously, she was Massachusetts' First Undersecretary of Homeland Security, serving Governor Deval Patrick. And today she is the Faculty Chair of the Homeland Security and Security and Health Projects at Harvard's Kennedy School of Government. She's a national security analyst for CNN. She is the author of a number of books, including the bestselling Security Mom, and was a finalist for the 2013 Pulitzer Prize for Commentary. Oh, and she too has a podcast, The Scif for WGBH in Boston, and she also advises public and private institutions on preparedness and response planning.

So, Rhea, let's start with you. And let's start with the Colonial Pipeline incident. And just to provide context and remind everybody, this network carries 45% of the fuel consumed on the East Coast, about 15% of total U.S. demand. That's more than the entire consumption of Germany for more perspective I think it meets the definition of critical infrastructure. So, give us your take on this. Sort of behind the headlines, what happened? But more importantly maybe what's the significance of what happened?

Rhea Siers (RS): Thanks Kevin. What we're seeing is almost the pinnacle of a trend we've been seeing for the last few years. So, ransomware, essentially locking up your files and making you pay for them later, has been around for a long time and it's become a cyber weapon of choice, especially among criminal groups. It usually brings a quick payoff. That's where they were looking for the most opportune target, one that's not usually aware of its vulnerabilities. What we're seeing now are two things. First, we're seeing something called double extortion which looks like they may have perpetrated on Colonial where cybercriminals steal the data before they encrypt it and then they threaten to release it if it has embarrassing information. That's also become a weapon of choice during COVID. But the thing that I think has alarmed everyone the most is we've watched criminal hacker groups become more and more sophisticated in their exploits and the way they get into your networks and your systems.

They've become more and more tenacious and persistent, which are the types of cyber behaviors that we usually use to ascribe to states. The other piece of this is that we've seen these cyber-criminal groups moving from information technology to operational technology, such as industrial control systems at Colonial and other places. And that's a concern as well. And the third piece is these groups do not necessarily stand alone. Sometimes they have active assistance or passive allowance from the states in which they're hosted or where many of their personnel are. And in the worst cases and

that's not necessarily true of the group that exploited Colonial, but it has been true in the past. We've even seen state intelligence officers for example, in Russia, go from their day jobs, doing intelligence collection, using cyber to their moonlight jobs of engaging in cybercrime. So, what we have is a series of hybrids that are arising, that are becoming more and more dangerous and more and more of a challenge to deal with.

KK: I want to get into that in just a second in a little bit more detail, but before I bring Juliette into the conversation, from what you can see or what you know so far was Colonial a particularly vulnerable situation just because of their own profile? Or is this a really cautionary tale that should be a wake-up call, or had they left the door open?

(RS): It's hard to tell right now exactly how the perpetrators got in and what they used. I think the thing that is alarming is most of these cyber-criminal groups, including the one that was involved in this, try to fly a little bit under the radar. I don't know if they anticipated that they were going to end up way over the radar. And I know Juliette can comment on that. In this particular thing, one would assume that they were able to either enter the network through let's be honest, human error or human issues, or they knew of a vulnerability that they could attack that hadn't been updated or wasn't even known to Colonial. Until we get all the information, we don't know for sure whether it's system vulnerabilities or some kind of phishing attack that resulted in this, but that's a piece we must have.

It's a cautionary tale except we've had so many wakeups in cyber that I don't know what else we need. I think we've been slapped around enough that we should know. And so, it's just another on the pile of what goes on. The impact of it of course, down the line is what gets the attention. And by the way, since the administration issued executive order last night really in response to the SolarWinds hack not this, we can see now that we're going to start having a basis for good practices starting in the federal government.

KK: Great. So, we'll get into that as well in a moment there when we turn to the bigger cyber picture. But since we're on the subject of ransomware Juliette, how do you advise? I understand there's different types of companies with different types of asset vulnerability and the like. But is there a general view here on the concept of ransom? And are companies that represent critical infrastructure like pipelines or hospitals and the like, are they particularly low hanging fruit to the criminals? Because even a short interruption, as we've just seen even a short interruption is potentially catastrophic.

Juliette Kayyem (JK): Absolutely. So, I mean, just think of the critical infrastructure. A disruption becomes a national security event for the United States. So, disruption in a private company becomes a national security event because it is critical infrastructure. So obviously the stakes are much higher. So I come from this from a pretty binary perspective and I know the arguments both ways, but I would find it very difficult to come up with a rational argument of why a company, once faced with ransomware, would be better off paying it unless the company's activities were nefarious or illegal. In other words, there's a whole series of ransomware going on among not legitimate organizations. That is, it's not that it's controversial. That is my opinion and is just one opinion only for two reasons. One is obviously you're just giving fuel to the fire. You are in other words. And the other is it does nothing to protect your own capabilities in the long-term just because word will get out that you've paid it.

We have some sense of what companies have paid and other hackers will go after you. So, I get it. And I think there's a reason why the Biden administration in their press conferences this week was not very harsh about companies that do pay ransomware, because we do recognize it as not legitimate, but maybe an easy way out. So basically, on ransomware that is it. I'm sort of surprised how big this got so quickly. And I, like Rhea am very, very curious about the after action for this company. Sort of what were their vulnerabilities? How did this get in? How did the entire system go down? How was that the only solution for the company?

KK: Yeah. And then on that point that maybe speaks more to corporate preparedness than it even does to the crime itself. I mean, it was almost farcical, the DarkSide response sort of like "Hey, we just wanted to make some money. We didn't intend for you to cut the entire East Coast off." I think we need to be clear the decision to shutoff the pipeline that wasn't that the cybercriminals had assumed control. It was the company itself shut the switch off, right?

JK: Exactly. Okay. So, they find out that the requests, we don't know all the details. But Friday becomes the day. So, this is, for people listening, this has been the sort of frustration for people like me who think about right of boom planning. So, Rhea is going to keep us from being damaged and once we're damaged, we'll try to pick up the pieces. So, if you think sort of right of boom, right that the bad thing has happened. So, I have a lot of questions related to this, and some of it may be structural. As many in the private sector know, corporations after 911 created this Chief Security Officer docket. And that's like normally a former FBI agent or a former police chief and they're going to protect the physical assets and make sure that we all do the fire drills and stuff.

Then with the internet and connectivity, then you have the rise of the CISO, the Chief Information Security Officer. I'm going to add a little and that was a different type of person. It was a techie person, maybe out of the security world, may be former secret service, but someone who came up generally whose expertise was generally different than the CSO. I'm going to add a little wrinkle quickly, what I'm starting to see in corporations, and we'll get to this later is the rise of the Chief Health Officer or Chief Medical Officer, because so many companies were caught flat-footed. But just going to the CISO and the CSO, they sort of live in different worlds. And I think maybe people are nodding. We have in here they sort of have, there's not a lot of connectivity.

You see companies trying to nurture that now because of cases like Colonial. One could not imagine, I mean, there'll be hacks that deal only in privacy and information. But for any company that has a physical footprint, the idea that the cyberattack won't have traditional security implications and vice versa is ridiculous now. So, you're starting to see some changes under titles like Risk Officer, Trust Officer who oversees both of them. And I think what you're seeing with Colonial is probably a dramatic manifestation of that division. Because for someone like me, it may have been understandable that they close it down on Friday because they don't know what's going on. But what I don't get is you said it was their choice. Did they not have a preparedness plan to mitigate the losses of a cyberattack?

To put it bluntly did they only have an on/off switch? It looks like that, right? So, what was the connectivity between the hack and their fears of the pipeline? I suspect there was probably information about storage and capability, real-time information about what's the capacity of the pipes? How critical infrastructure works. How much can you pump into a certain area that may have been taken. We don't know yet, but just for cyber

professionals, there has to be a lot more time spent on consequence management. You cannot assume that everything is going to be in the prevention stage. And it has to be better than an on/off switch because of things like critical infrastructure. Those are my big takeaways. I'm surprised at five days with an off switch.

KK: Yeah. I think the after-action on this is going to take some time, and it's going to be interesting. One last question on the ransomware front. Tell us a little bit about the rise of cyber insurance or cybersecurity insurance. And does that create a perverse incentive, or does that make companies more vulnerable since they're covered?

JK: Right. And Rhea may have something to add to this. Let's put it a different way. Every question you asked me about cyber, all I do is I think, "Okay, what would I recommend for physical?" In other words, my goal in the next 10 years is this pristine elite group of people who are super smart and know about wires and stuff. I think we didn't, how do you want to say it, we didn't nurture both the risk and consequence management side into an overall safety and security framework. And we've got to bring it back. And I think Colonial is a great example. If you're asking me would I buy physical insurance? Yes.

And I would recommend buying cyber insurance because to think that this ransomware activity thinks rationally about that, maybe they do, but my guess is that disruption at this stage, especially as Rhea was saying with the either tacit or explicit approval of a state sponsor, means that disruption is more important to them.

RS: I'd like to add something about insurance. I also think it's a force for good. I agree with Juliette about that. And one of the reasons it is, is because it could help you set basic standards for what you're doing, not just in cyber but also connecting, of course, to physical security and ensuring, for example, that your data centers are properly protected. But, it's the same thing for me as a homeowner. I get a discount if I have the fire extinguisher, right?

The insurers really have moved the market to those kind of prophylactic measures that are at least sitting there, and they also often review a company and let them know where some of their issues are, so from that perspective it's really not just an outstanding investment in terms of potential risk, it's also an outstanding investment in terms of preparation. And the big thing about preparation is your review needs to be agnostic. It can't be governed by marketing or other issues in cyber. It has to be governed by what you really need at that time. And sometimes that's difficult to find.

KK: You guys have done a phenomenal job of taking this specific incident and making some bigger points. And I want to broaden out a little bit further here. And maybe, Rhea, I want to dig in a little bit more on something you touched on earlier, which is DarkSide. Maybe tell us a little bit more about these types of organizations, generally. And can Russian-based cybercriminals really be separated from the Russian state in your view?

RS: Well, I think I'll start with the last question. I think it depends on the state, but I think when we're talking about Russia there are other things at work there in terms of how these enterprises interact with the Russian government that you have to take into account. And that makes it really difficult. It means we have an outlier. We talk about wanting cyber norms, and they would be wonderful to have that also include not attacking critical infrastructure, for example, but you're going to have to decide how you're going to deal with your outliers. And they are an outlier.

And a number of Russian and other backed cybercrime groups, or at least ones that seem to have a connection to operate out of Russia, have increasingly had industrial victims in their sights. They hit a bunch of them with ransomware. There was the first ransomware that was custom designed to cripple industrial control systems. These warnings have been out there. And we're aware of them. And we've seen, in a separate way, the Russian security forces use them against Ukraine and others. All that is out there. And trying to deal with that, I think, is a challenge that obviously private industry cannot do by itself. I mean, we've now moved to that national security level that Juliette talked about before. We have to be aware of that.

JK: Just on that point, I think to view Russia as the outlier, maybe North Korea, but the one thing I think about Russia is, does the organization, the criminal organization, feel that they would be punished for their activity. So, they don't need direct "you do this", right, but they're sitting there, they're about to do something with huge consequences, even though, as you said, maybe they were bigger than the DarkSide ever thought. The lack of feeling punishment is, to me, the state sponsorship. And, honestly, it's a little bit like Al-Qaeda in Afghanistan, right, that you're going to just work in a space in which the state is letting you do all your nefarious things, even if the state is also nefarious. That's how I think about it. Because I'm not in government, I don't have to be careful with my words. This is totally state sponsored, I mean, just because they know that they won't be punished.

RS: There's one issue here we talk a lot in cyber, and I'm sure some of the listeners have dealt with this before, about attribution, the who done it of cyber. Our focus on that, to find out exactly which server the attack came from, is a great thing, but it leaves in the dust this whole consideration that Juliette is talking about. Who's really involved? Who has control? Who has knowledge? And the fact that we sometimes immediately run to the technical data to look for that attribution, keeps our eye off the prize of how we're going to handle this.

KK: Yeah. And it's interesting because we're talking about the criminal element here so much, but there's obviously another side as well, which is the dominance of the space, right? Russia and its proxies continue to try to interrupt, continue to try to undermine. There are other countries that are doing that, but China, in addition to that, is also trying to dominate the 5G space. They're laying cable everywhere, etc. As David Sanger of the New York Times put it, "If Russia is the hurricane, China is climate change." And that leads me to this. It's very clear, as Rhea said earlier, how many more examples do we need to have pile up here, but we've proven the theories that came out a decade or so ago, what have you, that the battlefield of the 21st century was clearly going to be in cyberspace.

And by definition, therefore, the battlefield is going to be in the private sector as we have seen now time and time again. Companies have been dealing with theft. They've been dealing with ransom. They've been dealing with industrial espionage and the like, but, Juliette, are they prepared for actually just being the collateral damage in state on state warfare, effectively where just destruction or deliberate loss of control is the objective rather than something more commercial?

JK: Yeah. I think that the answer is no. I mean, that's too harsh, but what is likely to happen in this new stage of warfare, and I'm not going to be political, but one thing I will say is the move to the private sector hacks is consistent with looking at ways in which Russia and criminal organizations can disrupt the U.S. government outside of election, right? They've been exposed, right? 2020 showed that it was harder for them to do what they wanted to do.

This is now just the next wave, right? It was first elections, then critical infrastructure, and now it's the private sector. They're not ready. Part of it is they can't possibly be ready because they are not a government entity, so we do need the executive order that we saw yesterday.

Just to quickly just give the high-level bullets, basically, a lot of it is about transparency and information flow within the government. Part of it is requirements for contractors, which is key because if you look at SolarWinds and others, those were all done for the licensees, not the licensor, which was SolarWinds, which was less interesting to the hackers than the licensees, which were federal government entities. It's trying to do a unity of effort around cybersecurity, and that's on the prevention side. And that is great, and disclosure and information sharing, all the things that we need, and encryption and all this. What I urge the private sector in critical infrastructure is get real serious about, essentially, the Internet of Things. This is where we are.

The attack is on one side of the ledger and the consequences are now going to be physical because that's all you do. I mean, that's all these companies do is physical. And this is where all the wonky words that people like me and Jonathan Wackrow and others, who are with Teneo, think about is layered security, cascading losses, fail safe systems, all the wonky words that we know how to do this. But I think one of the things is people were siloed. Someone described it to me, if there was a big banquet table for cyber security, and you have risk, vulnerability, and consequence, lots and lots of fancy people on the risk side. What's the risk? What are we doing? Vulnerabilities, you've got people trying to protect, maybe fewer. And then the consequence side, where's your team? That's where I think the next wave is.

KK: Rhea, you alluded to something a few minutes ago, so much is made of the fact that when it comes to cyber warfare, there's no, let's call it for shorthand purposes, there's no Geneva Convention, right? Nobody really agrees on where the lines are. You referenced the challenge of attribution, of definitive attribution. And obviously, the richer and, therefore, more connected countries like the U.S. are more vulnerable than some of the attacking countries that have less to attack like North Korea or Iran. I guess, in your view and in the view of the intelligence community, I mean, are there red lines? And have any of those red lines been crossed?

I mean, one of the things that strikes me about the SolarWinds hack is that it looks really bad, but thus far it appears most of it has been surveillance and I mean, intelligence agencies conduct espionage. Big surprise. But, it's espionage until it's not. And we don't really know what the full impact of this is. In your view, have red lines actually been crossed yet?

RS: Well, I think red lines were crossed when Russia attacked critical infrastructure. And I do think there's a consensus, to a certain extent. There's even a huge manual that was written called the Tallinn Manual that outlines every possible thing that can happen in cyber. One thing people seem to agree on is once you cross into the damage of the critical infrastructure and cause human harm, you've crossed into an act of war. I think that even with what I called outliers before, it doesn't matter. You can have those norms, and they become a basis, but the interesting thing to me is not so much how states continuing to negotiate these, which they do ad nauseum at UN and other things, it's that the private sector and big tech in particular is talking about how they are going to support certain norms.

And they've now set up various organizations to talk about whether they should continue research in certain areas or to limit access to certain tools. That's an interesting thing to

watch, but I also think you're going to obviously see, in this administration, a continuation of previous efforts in the Obama administration to at least get some kind of rules of engagement agreed to. And even if we have countries or groups that don't agree with them, it still gives us a firm enough basis to move on. It's certainly worth it. And I think it helps the private sector by their understanding of what we consider the red lines to be as a government.

And I will say something about SolarWinds. It is definitely, I mean, no question, it's espionage, but it's not garden-variety espionage. It's very vast and very broad, I mean, just the number of victims, quite frankly. The question is when do you exceed what is standard intelligence conduct? And I don't think anybody can really answer that question because we don't want to. But the bottom line is at what point does it become so pervasive that you've affected the supply chain, your cyber supply chain, that attention needs to be leveled on that as well. And I don't think we have that answer yet, and I think that's another issue the current administration is dealing with. And that will also impact private industry as well.

KK: And what can you tell us, Rhea, I don't want you to obviously divulge what you can't, but talk about maybe the challenges as well of our ability to deter and our ability to punish, right? Right now, right, China is saber rattling over Taiwan as an example. So, one of the things that we do is we send carrier battle groups through the Straits of Taiwan, right? It's a show of force. It's a suggestion that we would be there even though there's strategic ambiguity around Taiwan, but we show what will happen essentially. Right? And that should deter aggressive Chinese behavior.

We don't really show, we don't really publicize, we don't really demonstrate our cyber capabilities. And also, once you punish, my understanding is there's kind of a one and done. You've exposed what your capabilities are, and you have to move on to the next tool. And, again, what's proportionate response to these types of events?

RS: So, we really don't have an effective cyber deterrent, and I think everybody understands that, and we've never been able to demonstrate it per se. But, you're right, we have this very difficult balancing act. What do you do to punch back in some cases? What's informative is looking at what the U.S. intelligence community and the whole of the U.S. government actually did in response to another potential round of Russian interference with the elections. They were very focused on it. They did a variety of things to stop it operationally, but also to expose it. It's a set of tools you use, not just one. But whenever you do punch back, you, of course, do show your capabilities. When you decide to pull out a stuck set, a cyber super weapon, even if it's successful, your adversaries know what you're capable of, and they can in fact parrot it very quickly.

So, one of the things you have to be concerned about is using the tools when you really, really need them. You have to have a prioritization. There was, in fact, during the Obama administration and Juliette, maybe you know this better than I do, a classified discussion on when you decide to respond. That is something that's been missing for the last few years, and I would assume that the new administration will go back to reconstituting, and they have some great people to do it.

KK: So, staying with institutional response here for a moment, Juliette, talk about corporate government relations on this front, right? Companies typically obviously want to have light touch regulation, but perhaps as we've just seen with Colonial, advisories versus regulations don't always seem to work, right? In the case of Colonial, the Department of Homeland Security set

up a pipeline security initiative in 2018, and in 2020, they warned but did not force pipeline operators to keep back office and operations separate, and clearly, now we've seen the consequences of that. So, what's the right balance and approach here? And it's especially challenging, is it not, for companies operating internationally who don't want to be seen as necessarily too cozy with the U.S. government for their own international reputation?

JK: Right. So, I think we're at a pivotal place on this, and you're right. Gosh, when I started in the Obama administration, we were talking about best practices certificates. That's as harsh as it got, like, "Oh, company you're doing really good." It then started to change over time. So I think this executive order from yesterday is the beginning, and whatever controversies or debates that were going on internally, they clearly got silenced by what happened with Colonial. So, one is a combination of carrots and sticks by the government. So, the first is sticks, because the executive order has a lot of sticks in it. It is going to hurt in the wallet for companies not to have at least some baseline capability and capacity and protections for their networks, because basically you can't even now be a subcontractor on a government contract.

So that's a lot of companies now, right? Where you're a subcontractor of Raytheon, you may have no interaction with the federal government, but now you're going to be encompassed in that. So that's key, and I think that's absolutely right because the back door has always been the problem. With Colonial, back door was not a problem, but in the past, the back door has been the problem. You can think of other sticks that might be used over time, like I would require, as we do with critical infrastructure, a regulated response and consequence management for cyberattacks. Require that as part of whatever sort of regulatory process there is.

But I actually think, in the same way that we think of offshore drilling after BP oil spill, and nuclear after Three Mile Island, we may actually be at a pivotal moment where the idea of not regulating the safety and the industry's networks will be viewed as very quaint. And so, people need to prepare for that. Maybe this will just be viewed as a blip because Colonial got their act together, was able to get back up and running, but two or three more of these and you're looking at cumulative impact. So, is this what Three Mile Island was for the nuclear industry? Stay tuned, but I wouldn't be surprised if it was.

KK: And just for the benefit of our audience who may not be as familiar with this yet, so what exactly is the executive order saying that came down yesterday?

JK: Yeah. Okay, it came down yesterday, so I'm going to do this from memory. So, remember, executive orders, people have to remember, can only apply to the federal government's own behavior. So, there has to be a federal government nexus. That's a difference between an executive order and a law. So, it basically requires same standards. It's basically bringing DHS and energy, all to the same standards of the Department of Defense in terms of encryption, data management and data sharing. That's good. Because DOD has always had the most rigorous one for obvious reasons. We just viewed that as more pristine. So, you're going to bring energy, well, actually every agency, but energy and DHS will be the most relevant because, remember, DHS, while not the owner of critical infrastructure, through its infrastructure security program is the, if you want to call it a regulator, the regulator of the industry.

The Department of Energy is more focused on capacity and are U.S. citizens going to be impacted by this? So that's the first thing in terms of internal review. Then the external is through the contracting system. So you can

do an executive order that way, that if you have a nexus to the federal government, you are now required to disclose certain information, to have certain baseline requirements that I'm just not going to get into the technicalities of it because I don't think it's been chosen yet. It's just basically a warning that things will come into play.

And then your licensees will also be subject to that. And to me, that may be the biggest part of this because of the backdoor problem, which was your big company was maybe better than the smaller company, but through the back door, they get in. I don't know, Rhea, if there was anything else big that I missed.

RS: No, I think you've covered it perfectly. And the idea that it's kind of "son of" the DOD contracting regs is really important. It shows that they worked and they're applying it writ large across the federal government. And, frankly, I think we both think it's about time.

KK: So, moving a little bit one step below the federal government writ large level, Rhea, talk a little bit about the challenges here between the corporate sector and the intelligence community and law enforcement specifically, right? Because, obviously, one of the things that we've seen is that there are disincentives for companies to either cooperate amongst themselves or even with the government and law enforcement because they don't want to divulge their vulnerabilities. They don't want to divulge what they've lost for competitive and reputational reasons, etc. So that's question number one.

And question number two then is the challenges, again, posed by what looks like happened with solar ones, right? You are at the NSA. You are supposed to be outwardly facing, right? And yet it appears that Russia infiltrated U.S.-based servers and then perpetrated the crime from there. So, from within the country, which makes it very challenging. I guess it's 911-like, right? Once the pilots were in the country, it was more challenging. The handoff had to occur, and so on. So, talk about these challenges.

RS: All right, I'll start with the private sector and the intelligence community, which when I say intelligence community, I mean writ large. I'm also talking about DHS and its specific cyber component. We have the basics there. The problem has been perhaps putting them on steroids at some point. The real problem is everybody throws their information over the transom to each other. Actually, there are these information sharing coordination groups. For example, for the financial sector, the retail sector, you name it, there's one. Some are more effective than others. The financial sector is leagues ahead of most. But the piece that's missing is actually trying to put all the pieces together. And since they don't speak the same language often, that could be difficult.

Now I've been on both sides, so I feel I can be fair about this. In the private sector, they'll provide information about attacks. They'll provide information about vulnerabilities that have been exploited. Sometimes they get feedback and sometimes they don't. It's a very inconsistent thing. And I still got the feeling sometimes that it was almost ad hoc, which I found to be frightening. On the other side of the coin, of course, the intelligence community is dealing with information that's perishable, either because of the source or the method. So, they're going to be careful about what exactly they throw over to the other side. That sometimes results in partial information or the fact, and I'll say this very honestly, that intelligence information is it's really its own school. And so, as a result, the people receiving it can't always understand it unless they have people who can actually analyze it.

So, this is the thing we have to overcome. There are models that work, and a lot of people have spoken about them. And, in fact, since we

keep talking about the Department of Defense, the defense industrial base, for example, is one of them were information is shared in national security issues for these companies that are very involved, obviously, in the national security sector. That has to become a more coherent. We're also dealing on the private side with a patchwork of companies. That's very true of utilities and it's true of even financial institutions. Big banks, big resources, using them really well on cyber security and then little ones, and evening out that playing field, I think, is a huge problem. Now, the second part of what you asked me about the domestic piece. So, this is a discussion that's fraught with peril, in my opinion. I know, and believe me, I'm a big fan of NSA, obviously.

I wouldn't have spent 30 years there if I wasn't. We have some of the best people in the world to solve problems there. Unfortunately, we're talking about domestic servers, and that is not the authority of the National Security Agency. And I would also suggest two things. One is I don't like the optic of an intelligence agency being involved in domestic information, so we have to overcome that. We have to continue to empower the FBI and DHS to do that work because, frankly, they're improving all the time. I don't like this atmosphere where we say, "If it's not NSA or CIA, it's not good." That's not how we should be operating. So, we have to ensure that we have the right people on the domestic side. And, listen, NSA and others can come in to help you on a case-by-case basis. And, of course, they have on certain things. But they cannot also assume responsibility for some of these things on a domestic level, because, guess what?

They still have a foreign intelligence mission, and they can serve that by looking at Russian trends and what's going on in terms of Russia, but they can't solve every problem that enters us domestically. And I know we used to call that "the wall" in counterterrorism between law enforcement and foreign intelligence, and I think it's great, Kevin, that you brought up the fact that that's still an issue for us now in cyber. We're going to have to find ways to do it where we can use the expertise that we need badly without sending a message, frankly, to the public that this is becoming part of a huge intelligence apparatus, which I, frankly, think just is not marketable.

KK: Yeah. It's really fascinating that something that was exploited in the analog world 20 years ago is being exploited today in the digital world, which speaks then not to the technical side but the structure of our society, that it is uniquely exploitable at the moment until we figure this out.

I mentioned a couple of times, and I want to come back to this, Rhea, is you talked about how the financial industry is kind of light years ahead of everybody, of many other industries. Is that because of heavier touch regulation that forces them to be so versus this light-touch regulation where we've seen just in this most recent example?

RS: I think they got slapped, frankly, and they took their wake-up call and ran with it as opposed to other industries. They had several wake-up calls early this century and some from the Iranians and others. And they realized they had an issue. You juxtapose that against where their obligations are. Their responsibility is to their clients, their shareholders, and to their regulators. So certainly, regulation and the fact that there are essentially cyber audits of financial institutions makes a difference, but this is also really an internal-facing priority for financial institutions.

They realize that and they're used to dealing with fraud. And I think that's also a big factor. Because they're used to dealing with fraud and crime, this also was a priority for them. And they've learned that they have to be as agile as the criminals. So, when they're well-resourced, that's what they do particularly well, but they

do it as a group. They do it as a sector. And I really think that's made a difference. It's not a perfect record. Nobody bats a thousand in cyber either, but it certainly shows that if you're willing to put the resources on people, process, and technology, which is what cybersecurity is, you're going to be in a much better place.

KK: My apologies for spending so much time on this subject but clearly, we're going to be returning time and time, again to these issues for years to come. But one of the lessons here is that clearly a lot of this comes down to preparedness, and I think that's a perfect segue here. Juliette, I want to turn right now and this is going to be like an abrupt record scratch to everybody I suppose. I wanted to turn to COVID here for a moment because right now, everyone in the country is focused on reopening and returning the economy. If anything, we're worried now about overheating the economy as we've seen market performance over the last couple of days. But let's be clear, the meta-point has been made here. There are infinite opportunities for pathogens to sort of make that leap from animals to humans.

And so, there are more pandemics to come in the future, not to mention all of the other low probability, but high impact, potential events. But companies and governments alike, they can't be totally prepared for all of them. And they can't be mired in just fighting the last war. So, what have we learned? What do we learn here as far as best practices are concerned for preparing for these types of events?

JK: Right. That's great. And I should say I spent a lot of last year, I like to joke that I was 25 and in 2020, aged doubly, but through the Bloomberg Mayor's Program, worked with a couple of hundred mayors, a bunch of governors. And then, of course, a lot of entities in the private sector, large retail, whatever. I'll tell you some of my takeaways, but I'm going to start with a pitch. I am also a columnist for The Atlantic and maybe Teneo can get this story out. I think that the public health messaging is not very helpful right now for industry and I wrote about that. And I think we're starting to now be a little bit smarter about how we talk about it. The public health people were constantly talking about this thing called herd immunity, but without talking about what was going to happen before, and if we got herd immunity.

It is clear now with vaccine hesitation that we've hit a wall, but it's also clear, people are more sympathetic. Vaccine hesitation is really movable and the anti-vaxxers are such a small part and it really does have to do with access. So that's why you're seeing governors come out with lotteries and beers and LL Bean is now giving away free stuff. I mean, just do it. Just figure out how you grease the runway. But the one thing I want to say for the private sector and a lot of Teneo's clients and whatever else is, this is also on you. And so, this is once again to the carrots and sticks. I'm not into vaccination punishment. I don't think it's going to work. I think given the communities that we have to move that it's not appropriate. It's just not. I know more progressive people are so angry about us not getting to some number that no one knows what it is.

We're in great shape, the numbers. And we need to say that every day as leaders in industry and public health. Hope is something people need to hear. It was a really crappy 18 months for a lot of people. But how do we get to better hope? And this is where I want people to think about the TSA CLEAR line and national TSA PreCheck, excuse me, which is, begin to think of the world as the burdened and the unburdened. And the unburdened. I like this idea of thinking about vaccination is unburdening you. And those of us who have been vaccinated, I think I underestimated that feeling of freedom after that second shot.

And so, it's unburdening you, and that means benefits will accrue to you.

So that's what the cruise lines are doing. And I think the cruise lines are going to go to vaccination only because as a commercial decision, they're saying, "Is the average cruise goer," that's not me, but I'm going to pretend like it's me, "The average crew, Juliette Kayyem, more likely to go with mandatory vaccination as compared to someone unvaccinated likely to go." They know what the answer is. And so, Broadway is doing the same thing. Is someone who's going to pay for a Broadway ticket, more likely to pay for one if it's vaccinated. But part of it is making it accessible. So, in terms of your employees, in terms of the rules that you set for admission, whether your sports, entertainment, hotels, whatever.

So that's my pitch as well because the private sector is going to be really, really helpful in essentially creating a world in which the burdened, those not vaccinated, look at all of us partying and able to go on cruise lines and going to Broadway and concerts and say, "That world looks better. All it is is a shot." And I think that's how we get there. And I'm not worried. The numbers are just too good. I'll let the public health people be worried. I'm not worried. Okay. So just very quickly on sort of then the path forward. So just three quick things having done this. One is just better situational awareness. Actually, this is similar to cybersecurity, where I was really surprised how unknowledgeable a lot of CEOs were about pandemic planning. And I remember telling a large retail CEO, "You're going to be closing down all your retail stores."

And he was like, "That's like telling me that Martians are going to land on earth." In March, people were surprised. This is the rise of the Chief Health Officer and the Chief Medical Officer. You don't necessarily need to do that, but just have greater transparency. The second is early decisions are better than late ones, even with imperfect information, but that requires leadership to have a very strong communication plan. I had always recommended a daily battle rhythm, at least through 2020, that leadership is constantly communicating with employees about the pandemic, not about work. Because in the gap, people fill in all sorts of craziness. And then I think the long-term lessons, obviously people are talking a lot about work, and women and work, and how we want to work, and work and kids. And find out what your employees want.

I mean, the idea that, depending on what kind of company you are, it is going to be a competitive advantage for companies who can offer more creative work situations. So, Goldman Sachs may decide, we want the traditional, everyone comes into the city or comes into the office. That's fine and that is their corporate decision, but a much, let's say less established company will find, "You know what? I do like that person in Denver. And I'm here in Austin. And one year ago, I would've thought that was impossible, but now I see that it is possible." So, find out from your employees because it will make a better work environment. And then just be ready to pivot again, if the numbers start to not look good. But this is my vaccination pitch, if the public sector sort of rode the wave, when Biden came in and sort of got us to the wall, I really think it's going to be the private sector creativity, the hand to hand combat as I call it for the stage we're in right now.

KK: Yeah. And we've seen the ability of even institutions to make these adjustments. It was interesting this week here in New York, that the city had made the announcement that there will be no more snow days in the future because the schools now can go to virtual learning on those days, much to the chagrin of children everywhere. But I think a lot of what you're saying comes down to, I think the great maximum of General Eisenhower about military planning, right? That when the first bullet flies, the plan

goes out the window and is worthless, but planning was everything at the end of the day. Well, we could go on, we could move into all-new subjects because there are many more that are relevant here, but I am aware of the clock.

And so that's why I'm happy that Rhea Siers and Juliette Kayyem are Senior Advisors here because now we can have them back on this call in the future. And I hope you will be in the near future. I want to thank both of you very much and thank our audience for joining us today. Our schedule is going to be interrupted a little bit. Instead of being back in two weeks, we will be back next Thursday for our next Teneo Insights call with the leader of Teneo Risk, actually, with Commissioner Bill Bratton who's got a new book coming out, which we'll be talking about. So, until then, thank you, everyone. Have a great weekend. I'm Kevin Kajiwara in New York.

JK: Thanks, Kevin.

RS: Thank you.

Teneo is the global CEO advisory firm.

Working exclusively with the CEOs and senior executives of the world's leading companies, Teneo provides strategic counsel across their full range of key objectives and issues. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other global corporations.

Integrating the disciplines of strategic communications, investor relations, digital advisory, diversity & inclusion, management consulting, physical & cyber risk advisory, financial advisory, corporate governance advisory, political risk advisory, and talent advisory, Teneo solves for the most complex business challenges and opportunities.

teneo.com