Teneo

Teneo Insights Series: Cybersecurity: At Greater Risk Now Than Ever Before

Teneo Insights / September 9, 2021

Conrad Prince
Former Deputy Head
and Director General for
Operations at GCHQ

Rhea Siers
Teneo Senior Advisor and
former Deputy Associate
Director for Policy at the
National Security Agency
rhea.siers@teneo.com

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

Alexandra Lager (AL): Good day and thank you for joining today's Teneo Insights Series. 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. Thank you for joining and welcome to the new season of Teneo Insights. I'm Kevin Kajiwara, Co-President of Teneo Political Risk Advisory here in New York city. I hope you all had the chance to enjoy at least a little bit of summer, and that you were able to successfully dodge all of the myriad risks out there of COVID and wildfires and hurricanes and floods and all the rest of it. But, today we're here to discuss another now very constant area of risk, and that is cybersecurity. As the U.S. and its allies withdrew from Afghanistan, one of the rationales was

that it would allow us to refocus on the very big global challenges of the century. The strategic competition with China, climate change, demographic and technological shifts and all of the rest. But with the return of great power rivalry, I think we see another kind of low grade, but very high stakes warfare.

And if cyberspace is the key area of contestation of the 21st century, then by definition, the private sector is the battlefield. And the stakes are high, potentially existential to enterprises and the jobs of their leaders. It's also an asymmetric risk with the richest and most connected countries and their assets the most vulnerable. But, also because hacking is so scalable. Essentially nobody is too big or too small to target. And in addition, countries via their security services are outsourcing, effectively, to private sector talent, not just for that arm's length deniability, but because by sponsoring, but not micromanaging, these hackers, countries force multiply their sophistication and strength. And also become more unpredictable for security agencies to defend against. The bottom line though, is that while we all fear the so-called cyber-Pearl Harbor, the new normal is one of small, but constant attacks that, like 20th century espionage, is just a never-ending game to defend against. My guests today have spent their careers preparing for and dealing with these issues and I'm happy to have them on. I'm happy to welcome back to the program, Rhea Siers. She is a 30 plus year veteran of the U.S. intelligence community and among her other positions, she was the Deputy Associate Director for Policy at the National Security Agency. She is a prolific writer on this subject and is the coauthor of Cyber Warfare: Understanding the Law, Policy and Technology. She's on the faculties of Johns Hopkins, George Washington University, and American University. She served as the Cyber Defense Strategy Executive at Bank of America. And she is a Senior Advisor to Teneo. Conrad Prince is the Former Deputy Head and Director General for Operations at GCHQ, which is the United Kingdom's signals intelligence and cybersecurity agency. Subsequently, he was the Cybersecurity Ambassador for the UK government. And today he is a distinguished fellow and Senior Advisor on cybersecurity at the Royal United Services Institute, which is the world's oldest and the UK's leading defense and security think tank.

I'm happy to have him on the program for the first time. And actually, since you both represent the world's or the Western world's premier signals, intelligence agencies, or represented, I should say, perhaps it would help our audience to set the stage. It might help them understand what differentiates these two agencies and their two missions, because correct me if I'm wrong, but they're governed by different statutory and legal constructs, that define how they can operate and that restricts how they can operate. So Rhea you're the lawyer here. Maybe you can explain a little bit about that difference for our audience. And what's significant about that.

Rhea Siers (RS): Well, I'll start with the American side with NSA. And, I'll yield to Conrad on GCHQ authorities. But NSA was always set up to be a foreign intelligence agency. In other words, we were targeting outward, overseas and those were our primary targets. This is of course a complicated business when you're talking about cyber and other modes of communication, because as most of you know, especially in cybersecurity, we have a lot of hosts of internet addresses that may be stateside. So it does get complicated. Although over time, I think we've created a regime legally, regulatorily, and just through practice to deal with that. But, there are issues.

And since we are coming up to the anniversary of 9/11, it's very much on my mind, I think, is the fact that we learned a lot of hard lessons from 9/11 in terms of the sharing of information, who we could share with. One thing that does not happen in the United States is that law enforcement does not task NSA.

NSA's tasking comes from both the Department of Defense, as a combat support agency, and also of course from the Director of National Intelligence as we prioritize intelligence. The question is how do you share information legally and usefully while doing all that? There are models, there are changes, but I think as everyone remembers, there's great sensitivity to what are honestly significant surveillance powers. And the need that many people see, understandably, to protect their privacy. So balancing all that out, both in terms of authorities and practice, and also understanding the way criminal law in the United States works, in terms of needing warrants to do surveillance, makes this a very contained and sometimes very complex set of powers and authorities.

KK: So then Conrad, in contrast, how is the GCHQ set up in the UK?

Conrad Prince (CP): Well, thank you very much. And thanks for having me today. It's great to be here. There are similarities and there are some differences. GCHQ is an independent agency, one of the three intelligence and security agencies in the UK. It's not a part of our Ministry of Defense or anything like that. So we don't have that sort of complexity of being part of DOD. It has, like NSA, it has both the intelligence collection mission and what we now call the cybersecurity mission. And that's expressed through the National Cybersecurity Center, which is part of GCHQ. And critically also it's a key partner in our new National Cyber Force, which is how the UK conducts cyber operations, which I guess we'll come onto in a moment. There's a very strict legal framework surrounding what we do.

There's a lot of oversight of what GCHQ does. But I think, in general, my experience is we have a relatively simpler framework than was my experience of working very closely, as I did, with our fantastic U.S. colleagues. It's much easier for us to share material information within government. We've got very close operational relationships with law enforcement, for example, as well as with our own forces. And so that's the framework in which we are able to operate. So some similarities, some differences. And, a strongly, highly regulated system and framework for operations.

KK: Rhea, you made the point at the beginning that the NSA was set up as a foreign intelligence service. And you brought up this pending anniversary of 9/11. And one of the things we all remember in the aftermath of that was once the terrorists were inside the U.S., it was a troubled handoff. They lost track of them. And then the disaster occurred. So let's get real world here for a second. Is there an analogy there? The foreign or the outward-facing orientation of the NSA, did that handicap the intelligence community's ability to detect SolarWinds? And correct me if I'm wrong, but the government really had no idea until commercial entities brought that issue to light. That, essentially, foreign maligned actors had gotten into the U.S. and then launched the attack from within.

RS: Well, first, I'm not sure we know whether or not NSA knows because there hasn't been a lot of discussion for obvious reasons about it. The fact of the matter, I think, as you indicated in the introduction is, many of the intrusions these days, and in this case, the supply side intrusion of software, comes in the private sector. And by the way, that's one of the reasons that there is a great deal of discussion right now on Capitol Hill on reporting requirements. So in this particular case, SolarWind, it's unclear 100% what went wrong, in my opinion. What I see in these situations and I've seen in some others, is the cleanup often falls to NSA. And now as well to CISA in the Department of Homeland Security to put those pieces together. Should they have been on top of it? I've heard a lot of different theories about why or why not they weren't. For me though, what rings true is I'm just not sure that NSA had access to some of the initial information.

KK: Yeah. I want to come back to government and security agency relations with corporations. We'll spend some time on that in a few minutes. But I want to turn to Conrad, because you brought up something a moment ago, in your role, you also oversaw the United Kingdom's national offensive cyber capability. And my question is, in general, are we, and when I say we, the Western democracies, are we really contesting disputed cyberspace adequately? And are we using persistent offensive engagement to stave off or deter these attacks?

I'm always reminded when the U.S., as an example, feels like China maybe threatening Taiwan. The response to that is to send aircraft carriers through the Straits of Taiwan. This is a direct signal and a show of strength to China or any other adversary, for that matter. And a reminder of what they would potentially be facing if they were to take a step, a step too far. How do we do that in cyberspace? Demonstrate how robust we are, but without revealing all of the methods and technologies?

CP: So, I think first of all, offensive cyber, so we're talking here about using cyber to disrupt or destroy, and have a real-world effect, as opposed to espionage. I think cyber is not great for signaling in the way you're describing it. And I think many academics who've looked at this and you'd be fascinated and would raise views, have concluded, it's not a particularly good tool to signal because of all of the issues that you've talked about. The essentially covert nature of it, the fact that it's not always clearly attributable, and all the rest of it. So that's the starting point. I think the second thing I would say is, for me, the advantage in offensive cyber is likely always going to sit with our adversaries because they are unconstrained by an ethical framework or a legal framework, and the kind of considerations that have to be brought to bear when looking at how you use these sorts of capabilities in the real world. We, however, have a strong, legal oversight, strong legal framework for what we do. We've got a strong ethical framework. We've got strong principles around demonstrating necessity and proportionality in terms of our actions in cyberspace. And that's always going to, quite rightly, be a limiting factor on what we can do in terms of how we're going to go against adversaries. However, that said, I think, and again, I mean, I'm no longer in government. I'm not in a position to comment on what's actually happening on the ground. But, clearly we can see the potential for using these tools to disrupt those who would seek to do us harm in cyberspace.

And I think to me, from the point of view of Western democracy, is that's probably the most useful application of these capabilities. This is not about turning the lights off in Moscow, in my view. This is about targeted activity to disrupt whether it's cyber-criminal groups, whether it's nation state associated groups who are seeking to do us harm, whether it's child exploitation online, to actually disrupt these activities online in cyberspace, by doing what you might call counter cyber. You can see the same way in which the potential of these tools to disrupt the ability of our adversaries to exercise command, and control over the internet, or communicate over the internet. Which obviously is a key factor in counter terrorism.

So I think these capabilities are valuable for us in those contexts. I think that it is right that cyberspace should not be an uncontested space for our adversaries. I think we have to be realistic about the application of them from the point of view of Western democracies. And we have to be realistic about the kind of issues of scale and capacity and endurance of effect that one can achieve. I think for me, offensive cyber is a precision capability that you can use, particularly if you coordinate it with other activities and other lines of operations. You get the timing right, then you can have a significant effect. But, it's very important to see it in that context and not imagine that it's a kind of red button that can achieve whatever you want across the internet, across the globe.

KK: Right. So the question here for both of you really, at the top of the call, I asserted that while no single hack is likely to upend the international order, but rather we're in this period of seemingly omnipresent digital theft, digital spying, digital influencing, et cetera. I guess my question is, do you agree with that and to the extent that you do, where do you see right now and in this immediate foreseeable future, where the biggest vulnerabilities are, particularly as it pertains to the private sector and what types of risks? There's been a lot of talk obviously about ransomware attacks and the like, but what types of attacks are you most concerned with now? And maybe Rhea we can start with you on this.

RS: Well, I do agree with you. I've always had a visceral reaction to the term "cyber 9/11." But we are experiencing this other impact, which is almost death by a hundred cuts, especially to certain companies and the amount of expense and resources that are needed to defend successfully. So I think we have to keep that in mind, the type of horror stories and attacks that you often hear people discuss are attacks on critical infrastructure. The question is whether those are imminent or whether those are actually part of our adversaries' short-term strategy. I don't believe that for most of our adversaries that's true, but we're always going to have some adversaries who really sit outside the international system, especially North Korea, for example. So given that and good contingency planning demands that you're prepared for that. That sometimes makes it difficult to deal with all the other cuts that are going on. The disruption of business, the theft of intellectual property. Those are also national security issues. Those are economic security issues as well.

So what I'm seeing and dealing on the private side now, certainly much more than I ever saw it on the government side, is an incredible improvement in targets, tactics, and procedures by cyber criminals. Now, once again, I have to qualify and say some cyber criminals seem to have remarkable connections with certain states, and we know many examples of them. They often start with Russia, but nevertheless, when I talk about cyber-crime, I'm talking about that type of activity. And even though people probably feel they've heard an awful lot about ransomware, especially in the last six months, the reality is that is in the sector that has, in my opinion, expanded. And it's really through this offering of ransomware as a service, actually selling services that are connected to being able to shut down your business. This is really allowed criminals to create their own scalable business model. And so ransomware attacks are no longer only achievable by those with the means to undertake them. They can be undertaken by a great number of additional groups. That to me is a bit scary. You add to that the general tenacity and improvement in tactics and then one further move, we've seen ransomware and certain criminal activity move from information technology, attacks on your data, trying to exfiltrate information, now to operational technology. That's what we saw in a sense, and I'll qualify it in terms of Colonial Pipeline and JBS and others, and so add to that, the fact that the criminals are also hardening their practices. In some ransomware cases, data was destroyed rather than encrypted, even after paying ransom and others are engaged in dual extortion. So all those things and their secondary effects like we saw in Colonial Pipeline, makes that the area for me at the moment that really concerns me and just the sheer skill of the adversary is really actually something to behold.

KK: Yes. Conrad?

CP: Yes. So I agree with all of that. I think for me, it's the scale and the boldness of the attacks that we're seeing, particularly over the last 12 months. If you look at the nation state attacks, so obviously SolarWinds even more so, I would say the Microsoft Exchange server attack by China, I think affecting was that quarter of a million servers worldwide. Done in a way that then enabled cyber criminals to piggyback on the back of the operation and exploit it themselves. So I think it's that boldness and scale. I think it's the targeting of tech companies, the world's greatest tech companies for these so-called supply chain attacks. So where attackers essentially go after a tech company and then get their malware through the regular updates that that company provides for all of its companies. So it's how you can hit thousands of potential targets essentially through one entry point. And that those entry points are leading American tech companies. That's quite a matter of significant concern, I think, and the fact that nothing that the West has done to try and deter the activities of Russia or China over the last few years really seems to have that much effect. I think also when we talk about states, we're seeing the bar of entry lowering. So you're seeing the coverage of the NSO group, Israeli espionage, this espionage technology, the availability of that to all kinds of countries. Really, just for a price, you can get some pretty sophisticated hacking capability.

And then on the criminal side, exactly as Rhea said, I think part of it also is this thing of seeing some of these criminal groups moving into almost nation state territory in terms of their trade craft, in terms of their capability. And so, say for example, another ransomware attack, supply chain attack using ransomware by criminals. So that sort of shift, as Rhea said, that increasing capability and ambition is very striking.

The other thing I would sort of reinforce really on the ransomware point is, what we're seeing as Rhea said is the operational impact on businesses. And this is through ransomware attacks on standard administrative IT. This is not sophisticated, complicated attacks on industrial control systems and all the rest of it. This is because inevitably businesses operations are completely bound up with their administrative IT and how their administrative IT works. And so this is not just about data being stolen and then held to ransom. This is about businesses not being able to function for a period of time as a result of relatively straightforward ransomware attacks on relatively simple administrative IT.

And I think it's that operational impact that we see, not just in the core commercial sector, but increasingly in other parts of the CNI, the attack on the Irish healthcare system, for example, a ransomware attack, which I think led to up to 80% of medical appointments being canceled at one point. These attacks having real impacts on people's day-to-day lives and on the day-to-day ability of governments and businesses to function. And I think that's a really significant issue for us. And I think in terms of how companies are thinking about this, the resilience dimension is essential. And increasingly you've got to think about this as, when not if, how do you build resilience into your operations? How do you respond when the worst happens? That's got to be the way of thinking about it, I think.

KK: What's sobering here is that the picture that both of you have painted is every bit as daunting as media reports would suggest. In other words, media can oftentimes be somewhat hyperbolic about risks out there, but I think you've painted a very chilling picture. But one of the things that you're both talking about is how companies in the private sector, how companies ought to be preparing, how they should be defending themselves, what they should be preparing for, and then what governments and so on are doing.

But I'm wondering about collaboration on this front, because one of the things that we have seen over the last couple of years, particularly in the wake of the pandemic is with regards to the vast supply chain of physical product, whether it be semi-conductors now or PPE at the beginning of the pandemic, or we see something like the blockage of the Suez Canal, or all of these container ships that are trying to get into ports because of logistical challenges. The chokepoints of the global supply chain are incredibly narrow. We are reminded again and again, but those supply chains are company after company, after company, along the way and country to country, to country along the way. And so the interruption of that global supply chain is something that has profound—and we've seen it already very discernible economic impact, whether it be China, the German auto-industry or products being sold in the U.S. Considering all of the actors that are defending, how do we get them coordinated on an international basis? Or can we, is it just every man for himself?

RS: I would say we're beyond the every man for himself stage. There are a great number of multilateral efforts to try to share and combine information and protect certain parts of critical infrastructure. I think you're always going to have to acknowledge that some people are not going to play by the rules, and we know who most of those countries are at this point. But I think the problem we have had is prioritizing. And I think within the U.S. the problem we have is, it's been a tremendous challenge to figure out how the private and public sector are going to work together and how far the U.S. government can go to assist them in some of these things. And until we figure out those pieces, which I think is a prime goal of the current administration, at least hopefully it is, we're going to continue to have some of these issues over and over again. First, we haven't prioritized. Second, we move in and out of different norms, international norms created in terms of infrastructure and other things. And I think we follow the attack. Cyber traditionally has been very reactive, and the reality is that's just not something we can do anymore. As Conrad said, if you're not focused on resilience, which means preparation, no matter how you spell it, then we're going to continue to fall behind, be reactive and be picking up the pieces.

KK: Yes. Conrad, anything you would add to that?

CP: Clearly this sort of macro level, this whole supply chain, the globalization of technology, China is a sort of the fundamental challenge of all times and for the future. And you know that in the UK, the UK government has reframed a lot of its strategy around this, around technology, around how we develop approaches. That means as far as possible, we know we have sovereign technology industries and how do we protect those sovereign technology industries, particularly in key areas like AI and quantum, the usual things that people talk about. Then if we can't do that, how do we collaborate with trusted allies and partners to build our own technology? And then finally, if we have to rely on, shall we say untrusted sources, how do we then assure ourselves of the security and manage the security risks that come in that? Because given the nature of China and China's growing technological power, we have to find ways of working with that. And we have to find ways of managing those risks.

So I think this is sort of the macro geopolitical, technical issue of our time. I think in terms of government and the private sector collaborating, I think clearly that is fundamental. This cyberspace is an area where actually government, relatively speaking, is not necessarily that big a player. This is the realm of the private sector, at large, and government levers of power and control are not necessarily that great. You've got regulation and things like that, but not hugely. So I think that collaboration is essential. I think in the UK, certainly we see some good examples of that, particularly in financial services as you'd expect. So the areas that have been investing heavily in cyber for a long time, who have built up trusted relationships across the sector, who've built up trust with government. And so we've got good collaborative examples there that we can point to of government and the financial services sector working together on cyber challenges. We need to build that out across the critical infrastructure.

And I think one of the areas of concern for me is it still feels like financial services is a real outlier in terms of their investments in cyber, that focus on cyber. When you start moving into other sectors, which we would still call critical infrastructure sectors, there's quite a way to go still, I think. And government has a role in enabling that and in incentivizing it and requiring it through regulation in some cases.

KK: So there's a number of things to unpack here. And I want to get to that now, but just out of curiosity, we've been talking about these ransomware attacks, Rhea, you mentioned a few of them that have been prominent of late and other major hacks. And we're talking about them in the context of the U.S. or Western economies being the targets. But just out of curiosity, do we ever see any of this going the other way or Chinese companies, Russian companies, and the like, are we ever seeing them targeted in a similar way, or is this really a one-way street?

RS: There are some indications. On occasion, you see little glimmers of information. For example, the North Koreans who were really mentored in cyber by the Chinese actually may have attacked some Chinese banks. The question is, how did the Chinese respond to that? We don't know those answers publicly. And so every once in a while, you'll see a blip on the screen of this. Now let's just assume that criminal activity goes on no matter what, right? The whole question becomes; how are the responses from the state? And I think we could probably guess that it's somewhat draconian in both of those instances. But of course it still happens. And of course you have rogue groups who do other things. Just the tenacity and the targeting, and really the incisive way of targeting is just something that at least publicly, we see more targeting the West.

KK: And do you think that's because it's so much more fruitful to target the West or are we not draconian enough in the response?

RS: Well, first of all, if we're going to actually try criminals, we need to be able to extradite them to this country. I mean, it's one thing to issue indictments, which are useful tools in some ways that we've seen against certain Russian groups, certain Chinese group, Iranian groups, North Korean groups, but all we're doing as one of my friends likes to say, the only thing we're preventing them doing is these individuals can never come to Disneyland. I mean, we're really not doing anything beyond that, except educating and showing our adversaries that we have the goods that we know what's going on. So this kind of whack-a-mole situation doesn't really work. The question is, is there a way to address criminal activity overseas in the

United States? And the answer is not really in certain instances. Of course, with our allies and those we have expedition agreements with, it's entirely possible. And of course, it's occurred, and we have picked up a number of people, including some famous Russian hackers, while they were on vacation overseas and tried them. But again, what's going to be your emphasis? It has to be, I think they're calling it an "all of government response" in the United States. So it's not just the Justice Department, but they're part of it as well. So I just don't think there's an easy answer. And draconian measures probably are not as important to the United States at this point as finding some way to maintain good standards in terms of even cyber basics at this point for some companies. So it comes to the area, what are you going to emphasize? To me, it's worth emphasizing our resilience and our defense.

KK: So I want to go back to this subject of government and corporate relations on this front. And Conrad, if we may try to paraphrase a little bit about what you were saying a minute ago, private companies essentially build the architecture of the digital world and they generally facilitate that flow of data. So to some degree, the public authorities are kind of at the mercy of this outsized power. So talk a little bit more if you could about government and corporate relations on this front. Here in the U.S., we have seen President Biden's May executive order. We've seen the national security memorandum in July, but where are we getting on this front, either in the UK? And to the extent you can talk about Europe more broadly, but also in the U.S?

CP: Sure. I mean, I suppose there's many different dimensions one could talk about. I mean, it's worth just hovering on the nature of the transnational U.S. major global tech companies and their role in the internet. And clearly, we are in an era where these companies are supernational. They are above nation states. And I think there are some very challenging relationships between governments and between these sort of major tech companies around issues such as privacy and that sort of thing, which are really quite complicated and hard to handle and very different perhaps than from the kind of things we've seen in the past. And I think fundamentally, we're looking at companies who their marketing privacy, privacy is a core part of their offer, and that raises challenges for government, but there's no easy ways through that.

I think more broadly, looking at it from the UK perspective, clearly the key issue for us is our critical national infrastructure is primarily in the hands of the private sector. Chunks of that critical national infrastructure have still not achieved the kind of standards that we need, even the basic standards that Rhea was talking about a minute ago. So what does the government do to change that? Now for 10 years or more, we've been doing information sharing, we've been doing encouragement. The government's being much more forward leaning in terms of being able to share knowledge, share information, provide advice, and do all that sort of thing. I think that's been great, but even that isn't going to move the dial sufficiently. So I think we are seeing more regulation here.

And in the UK, we picked up GDPR and we picked up this thing called the Networking Information Systems Directive, which is another EU piece of regulation, which is targeting critical infrastructure companies and setting cyber standards for them. I think we're moving that agenda forward in the telecommunications sector. And I think that we'll see continued use of this regulatory lever to try and force standards up across a wide sway of the private sector in the critical infrastructure.

And that's quite an attractive tool for governments because as I say, they don't have that many levers to pull and regulation is one of them, but it's a double-edged sword. Regulation, if it's not brought in intelligently, if it's not brought in, in a way that really focuses on how businesses work, then it can get in the way. It can create perverse incentives. It can focus attention on actually areas that in the grand scheme of things aren't the things you really want to be spending your money on to improve your overall security posture. You need to have regulators, regulatory bodies that have the skills and the knowledge and the credibility to be able to enforce that regulation and engage with the private sector companies that are being regulated in a sensible debate and sensible discussion.

So it needs an awful lot to make it work. And fundamentally, I think regulation as a tool works best in big, relatively well-off sectors. So financial services for the most part can absorb the impact of regulation and can deal with it. You're looking at sectors that are much more made up of small to medium enterprises is much, much more challenging. So I think that that relationship between government and the private sector, that the way that regulation figures in that is it's an important part of it. It's a critical part of it, but it's really got to be got right. And there are a number of challenges in doing that. I mean, alongside that of course you need to carry on with information sharing. You need to carry on with the advice, carry on with the engagement, but that's only ever going to get us so far I think.

KK: You've mentioned a couple of times that financial services, and I think primarily you're talking about the banks and the large investment banks and the like being sort of outliers here. And hopefully, Rhea as coming from that world as well would affirm and attest to that. But what happens when a sector like that starts to move beyond the traditional business? And I'm thinking right now of the ever-increasing crypto element that's coming into finance, right? Where clearly people in the private sector or let alone in the regulatory sector or at the central banks and the other oversight bodies have a real understanding of where things are going on this front. But it seems to me it's a huge potential target. So what happens when an industry like financial services starts to move beyond what has traditionally been under the regulatory umbrella and how do we protect the bend or are we just dependent on them, Rhea?

RS: That's a really great question. I do think, especially in the financial sector, there is an ability to expand that regulatory umbrella pretty well to some of the cryptocurrency and other new models of financial institutions that work so differently than banks. I think that there's two keys here. One is whether we like it or not, we have to demonstrate that there are benefits and burdens to the regulations. What I mean is kind of a carrot and stick approach. So we have to demonstrate that there are advantages and that could include, of course, things like additional information coming from DHS or the information sharing groups that we've seen develop in the financial sector and other sectors. So I think that's one thing, and I do think there will be a huge push for regulation in the cryptocurrency arena, not just because we need regulation, but also because of the involvement of Bitcoin and other things in ransomware.

So those things are going to converge and they're going to have to be dealt with. But I think the key thing is that we have to demonstrate that basic standards, even the very most basic things in terms of cyber hygiene are advantageous to these companies and their clients. And that's how we bring them over the edge. I'll recall that in New York, the Department of Financial Services dropped an incredible number of requirements on chartered financial institutions in New York. It caused a huge response and it wasn't particularly positive from companies, but the practices that they were pushing for, things like having a Chief Information Security Officer, mandating penetration testing, those practices, if they're encouraged properly, might work in that kind of framework. And I really think you have to speak in a united way from the federal government to say, here are our expectations of the behaviors that have to occur, and if they don't occur, this means we have to dig deeper in terms of regulation. And we already know what it's like to be a highly regulated industry from the rest of the financial sector.

KK: So I want to bring together two things that both you and Conrad brought up. So Conrad was talking about the regulatory toolkit that governments have, and that can be highly effective in some cases. Earlier, Rhea, you talked about how a lot of companies still need to do just the very basics of defending themselves. And I think we all thought it was quite the wake-up call. I know, perhaps not all of the details are public out there, but the Colonial Pipeline supplying as much of the fuel needs of the East coast as it does was sort of shockingly vulnerable in a way. But talk a little bit about this balance because regulations can be good, powerful. It definitely defines the rules of the road to a certain degree, but there's a lot of bureaucracy there.

And there is also the regulators are then overseen by elected officials who oftentimes are not the most digitally literate in the world, as we have seen time and time again in congressional hearings, as an example. So talk about this balance between regulation, sort of voluntary compliance or industry-led standards, which can also be kind of self-indulgent in their own way, versus market pressure to push companies to take actions and say either via the way they're being rated by analysts and ratings agencies and the debt rating agencies, but also their ability to get insurance against cyber-attacks. How's that balance playing out right now?

RS: I actually think the cyber insurance industry has probably done more to bring companies to the right standard than maybe many other things. And so what they're offering of course is insurance, but on the basis of certain practices. I always compare this to 'I get a cheaper rate in my house because I have a fire extinguisher.' I mean, that's how it all started on the cyber side. They set out what they consider to be best practices. And they use that to determine what it's going to cost. But beyond that, they're indulging in some other activity that I think is interesting, including supplying negotiators when ransomware hits. Providing and in some cases, even providing information or resources to expand a company's cyber capabilities. So I think they've actually had quite a large impact. And remember they started from kind of ground zero in terms of being able to measure potential loss here. I mean, it really was so outside of everything they had looked at in business insurance up to that point. So that builds up on that. And in some cases, some people are critical of this, the fact that insurance companies have actually partnered with tech companies to provide protection and protection packages, all very positive things. I still believe that ultimately, in terms of standards and regulation, there has to be a carrot. And right now those are some of the things that are being considered in some of the legislation. Some of it is like limited immunity, some protection from liability. I think that's going to be potentially a big force in the market. And then the other would be that I've heard mentioned quite often is the sharing of what is called sensitive intelligence, which would be very familiar intelligence to both Conrad and I, with companies. That's a completely different set of issues, but I think it all goes back to the fact that you do believe it or not have to make this palatable to certain companies. Now, we already know in the financial sector. They've moved beyond that. But bear this in mind, I mean, the regulatory regime that any financial institution has to go through is immense. And that's not even in cyber. We call this other piece in terms of that as well. Everybody needs experts to do this work. And if you check the ads, you'll see that, for example, the Securities and Exchange Commission are always looking for cyber auditors, right? So this kind of gap we have in terms of the skills we need affects things here as well. And we have to be realistic of what we ask companies to do when we know how hard it is to find the right people, to, for example, harden our defenses.

KK: Right. Conrad, for a firm like Teneo, a lot of our clients are global multinational companies. And so they're in a lot of jurisdictions and they're attempting to do business and they're attempting to profit in a lot of different parts of the world and open a lot of markets. So talk about the downside of companies working closely with governments and security and law enforcement services. We have seen here in the United States as an example, that companies that can be branded as too close potentially to, say, Chinese security services or the Chinese military. And I'm thinking specifically of ZTE and Huawei, of course, but there the list could go on. They've essentially been run out of business in the U.S. and they are even having a challenging time doing business in China.

But the opposite can be true as well. If you're seen as too closely aligned with the U.S. government or the U.S. security services. Or in the UK, as an example, Tesla has just had to explain why the camera in the car in China is not sending data back to the United States. And yet that's the largest car market in the world. So it's important to them as well.

So how do we balance this now? Particularly in a world where we can no longer sell this notion that anything that the U.S. or the UK does, we're in the all-good. And the Chinese companies are operating in the all-bad environment. It's a lot grayer than that from a consumer and corporate partner perspective and investor perspective.

CP: Yeah, well, there's plenty to go at there. I suppose I would start by saying, I would say this wouldn't I, that of course there is a key differentiator in the sense that our government agencies involved in this work are subject to a robust legal framework. They do have independent oversight. There is a democratic system that underpins what they do. And that is very different from China or Russia. And I think that, inevitably I'm going to say this because this is the world I come from, but that is a fundamental difference. And it is a fundamental factor in everything that our agencies do. So that does make it different I think.

I think the Chinese case also is slightly different in the sense that, we can see a clear Chinese strategy to utilize technology, working through Chinese technology companies who will have very close relationships with the government, to use that, whether it's through the Digital Silk Road or the Belt and Road initiative, whatever you want to call it, as a means of expanding their global influence and global power. And that's absolutely clear. And that's not necessarily about having backdoors in technology or anything like that. That's simply about the provision of technology infrastructure, communications infrastructure, to countries across the world at a very, very cheap rate that then gives you, China, as the country providing it, a great deal of influence and a great deal of control over what happens around all of that technology.

So I think that is very different from the environment we're looking at here where I suppose from my point of view, I would say it feels to me like the big tech companies feel quite distinct from government on the Western side. I think, as I was touching on earlier, the challenge is to make that collaboration work when the tech companies and our governments are coming from rather different starting points around some of these national security issues.

So, I think there are differences. I think we can't just say there's an equivalence, that we're all the same and we're all as bad as each other. I just don't buy that. I don't think that's the case.

But clearly companies have to manage some of the presentational aspects. I suppose all I would say is that in terms of security, there are significant advantages from collaborating with Rhea's old organization, CISA, with our National Cybersecurity Center and so on, and being part of the solution. Because for us, I strongly believe that our solution to the cyber threats, the security threats we face needs a whole of society response. It needs the private sector and government and the individual citizen working collaboratively and working together because of the complex nature of the challenge. And so we have to have that collaboration. Now managing some of the external presentational consequences of that I recognize is an issue. But I do think the bigger game is in how we can bring the different aspects of private sector, government, individual citizen together to give us a stronger and more robust defense against the threats we face. Whether they're criminal threats or threats from hostile nation states.

KK: Yeah. I think one of the things that companies need to think about is exactly what you're talking about, the very real issues and the very real differences on the one hand versus the all too easy way of using social media and fake news and all of that to just put in the mind of the consumer that this company, company X, is dangerous for some reason. Which can have nothing to do with national security and everything to do with just the competitive environment. And trying to tilt the balance of how you message against that is going to be critical.

Rhea, one of the things that governments have found, and the U.S. government in particular has found, challenging in many ways over recent years is that setting red lines are very double-edged swords. On the one hand, they are useful. It is a clear message to a would-be adversary, do not cross this line. However, there's another message. Which is, if they do cross that line, you have to take action to maintain your credibility. We saw that problem in Syria for President Obama as an example.

But the other message that is received by the adversary as well, I guess I can walk all the way up to that line then without consequence. And so when President Biden tells President Putin there are 16 sectors which are the red line sectors, you cannot attack, you cannot go after. Does that suggest, and if you're a company that's on the other side of that line, that the U.S. government doesn't view you in the same way, or isn't going to defend you to the same degree? Or what's the message, what's the takeaway?

RS: Well, aside from the issue of using red lines, using red lines means you have a coherent deterrent policy to support it. And I think Conrad referred earlier to being able to signal and be able to let your adversaries know what your strategy is going to be, overt and covert, when a red line is crossed. Those consequences should be clear of course.

So what happens to the secondary? And I'm not belittling them, I'm just saying everything up to the line. The Solarium Commission, which was a bi-partisan group that issued a really expansive and good study, they call it the second declaratory policy. Which is a nice way to say what the Department of Defense has already said, which is called the 'defend

forward.' That means that you are prepared to counter and impose costs against specific adversaries' cyber campaigns, even below the red line. The cost is going to be different obviously than that major red line, but it's going to represent, resolve, and consequences. That's the essence of that policy.
Part of the problem here is I don't think we publicly see when that occurs. We don't see when the U.S. and its allies disrupt a significant disinformation campaign, until we hear about it later of course. We don't know when the U.S. interrupts a criminal campaign or something that crosses the line between state and criminal action. We just don't always see that. Sometimes we see it in the end in the indictments. But we don't. So there's just not the cause and effect.

The other problem there is, as you mentioned, we have 16 different sectors in our critical infrastructure, and we're loathe to prioritize which one we're going to focus on. Because we don't want to show that we're not focused on something else. The reality is our adversaries know where we're focused often. And sometimes we just have to bite the bullet for that 'defend forward' policy. It means we can't do everything, but we have to define what we can do, and how far we can go as a national security matter to the private sector so that they understand that the red line isn't the only border.

KK: And we have just a couple of minutes left. So I want to ask you both a very quick question if I could. Which is, you've both set out a lot of the risks that companies are facing. We've acknowledged that there's a very diverse corporate base in both the U.S. and the UK, big companies, small companies, internationally focused, more domestically focused, critical infrastructure, and not so critical.

But in general, as you advise a lot of corporate clients, and let's just focus on the ones that are going to be more typical of the audience that's on here today, which is going to be large, publicly listed companies for the most part, where do you find you're spending most of your time in terms of advising them? Where are you on the spectrum for the most part, if you can distill it down of helping them right now?

And I'll hand it to both of you, maybe Rhea, we can start with you, and then Conrad, you can have the last word today.

RS: So quickly, what I see is a lot of these companies really do have so many things in line. We talked about the financial sector and they have that. It's easy to get fatigue, I would almost call it resilience fatigue. You have to work on overcoming that. But the other piece that I think is problematic is the inability to speak across the enterprise in a language that everybody can understand.

And finally, communicating cyber risk from the frontline in cyber to the folks who are looking at the potential business outcomes from that risk. That communication is sometimes muddled, or it takes too long, or it's too late in coming. And I think it really does hurt some companies from being the best they can be.

CP: Yeah, I agree with all that. I think key things are cyber is never done, you can have a big uplift program, but don't think of it as something that you invest in for a period, and then you don't need to worry about it anymore.

I think in terms of specific issues, the supply chain risk is a really critical issue that a lot of companies are spending a lot of time on. I think looking more internally, there is a thing about cyber, everybody's got an accountability for cyber across a company, and it's getting it away from being something that's owned by a security organization or an IT organization, but mainstreaming that sense of ownership of the risk and accountability for the risk.

And I think when you've got companies developing new digital capabilities, doing a lot of DevOps work and so on, it's how do you build security? How do you build cyber into that work? So it's kind of the principle of security by design, designing security in from the ground floor. So you didn't have to try and retrofit it later when everything's gone wrong. But getting it in there from the start is really critical. And as we're developing new digital products and services, doing that in an efficient and effective way, I think is really critical in an ever-growing number of sectors.

KK: And not to put too fine a point on it, but exactly what both of you are talking about, this coordination of effort across the enterprise and how that is then messaged out is something that Rhea and my colleagues in Teneo Risk, the division that's led by Commissioner Bratton and Courtney Adante, this is exactly what they work on.

So if you have any questions on that front, please don't hesitate to reach out to us. So Rhea Siers and Conrad Prince, I want to thank both of you for joining me today. I want to thank all the rest of you for joining today as well. We will be back with the next episode of Teneo Insights on September 23rd, two weeks from today. The German elections will be that following weekend. For the first time in 16 years, there will be a new chancellor in Germany once government formation occurs. And we'll be focusing on the role of Germany in the world, and the legacy of Angela Merkel. My guest is going to be the noted author and journalist, Kati Marton, whose definitive biography of Angela Merkel called The Chancellor is coming out next month. And Carsten Nickel who runs Teneo Political Risk's coverage of Germany and the European institutions will be my guest as well.

So please join us then. Until then, Rhea and Conrad, thanks so much, thanks everybody and have a great day.

Teneo®

Teneo is the global CEO advisory firm.

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.

Teneo's clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations. Integrating the disciplines of strategic communications, investor relations, restructuring, management consulting, physical & cyber risk, financial advisory, corporate governance advisory, ESG, DE&I, political & policy risk, and talent advisory. Teneo solves for the most complex business challenges and opportunities.

teneo.com