Guidehouse

outwit complexity™

Parochial Views of Risk Leave Agencies and Companies Vulnerable:

Megatrends Video Series

Tom [0:08] Welcome, and thanks for joining us. My guest today are from the left to Patrick McArdle, Maryanne Bailey and Rodney Schneider. They are all partners at guidehouse. It's good to have you all with us today.

Marianne Bailey - Guidehouse [0:17] Thank you, again, great to be here.

Tom [0:19] And everybody, federal agencies, commercial companies, federal contractors seem to be operating in a ever increasingly risky world, cyber risks, this kind of risk, climate risks have so many risks. You see airplanes shot out of the sky. I mean, it's really risky these days. And so we're going to talk about the idea of operating in an era of increasing geopolitical risk, so that you can simply get your job job done doing for your customers doing for your constituents. And so let's begin with the idea of geopolitical risk. What is it? How do you look at it? What's a good way to view it? How should we consider it nowadays?

Marianne Bailey - Guidehouse [0:56] Great. So geopolitical risks are very complex today. And a lot of our clients don't really understand those complexities. And one of the things that we do as we work with them is we help them to understand this complexities. So whether they're looking at things like technology, whether they're looking at supply chain, whether they're looking at economic risk, they really need to understand the environment that they're operating in. And each one of those areas, you know, we can talk about them in detail, but they bring their own complexities with them, and us working across a broad set of clients. And across the globe, we get to see these risks, and we get to understand them in detail. So we can bring that understanding, and then we help our clients, you know, deal with them understand what they're dealing with, how do we break them down? And how do we help them address them.

Rodney Snyder - Guidehouse [1:44] So whether it's cyber, or the digital domain, even more broadly, or whether it's terrorism or for instance, war, but also whether it's things like sanctions and fraud, there's so much going on in the environment today, geopolitically across the globe, for governments, for private sector companies, for that sort of regulatory environment in between, that we really believe our clients need to understand, assess, and then be able to address that that environment, and therefore be most safely able to operate most profitably be able to operate, most optimally be able to operate.

Tom [2:21] Yeah, Pat, this seems like almost like the flowering of a trend that my memory started with the oil embargo of the 19, early 1970s, I guess it was when suddenly supply chains pricing, all the predictable industrial certainties that companies knew were not true anymore,

Patrick McArdle - Guidehouse [2:41] be the way our governments operate, especially the US government imposing sanctions, impacts commercial environment. So again, sanctions that our government imposes are a variety of things, they can be economic, they can be commerce base, they, they can be diplomatic, so So how they affect companies that operate within the United States, and as well as US companies operating outside of the United States. You know, that's something you need to be aware of. So the mere fact that I'm a US company operating in another country does not mean I'm not subject to the sanctions. And I need to, you know, take that into account as I execute my operating plan

Tom [3:24] will give us some examples of how this is operating right now. So everything

Rodney Snyder - Guidehouse [3:28] from economic sanctions on countries like Russia, of course, but also export controls, and then sanctions against individuals, individual companies, other entities. But you can find it in other ways, too, Tom, for instance, when it comes to foreign investment, both inside the United States, that now is covered by even greater sort of rigor when it comes to the Committee on Foreign investment in the United States and views, or whether it comes even increasingly, to US investors investing abroad in places like China. And then all sides are putting on more and more sort of controls restrictions on what can be produced and what can be provided to others. So for you see this, especially in the semiconductor field, where not only are there restrictions on semiconductors themselves, particularly certain types of quality, but even the equipment to manufacture those. So all of these things sort of come into play. You see China, for instance, most recently putting on some restrictions on minerals. These are metals that are found in the field that are very important to not only semiconductors, but also for instance, to developing other types of technology, including, for instance, solar technology. And so China's restricting that to make sure that not only do they have enough, but that they can control as much as possible what's going on in the world, just like we're trying to do when it comes to China's session in terms of that sort of technology and how important it is cutting to a previous conversation you've had about things like AI, generative AI and other types of ways is a really producing sort of even crater manufacturing and national security strength?

Tom [5:05] Yeah, so these are derived from a number of sources, including policy of the governments and governments themselves, as well as issues that are beyond anyone's control. My guest might say, and we're gonna get into some of the specific areas, but in general, companies, agencies, your clients come to you, and they're aware of these risks, sometimes, well, okay. So yeah, that's the question is, how do you prepare them for it, if they know about it, and especially if they don't know about it,

Marianne Bailey - Guidehouse [5:33] right. And, and that's kind of that's kind of our job. And that's where we come in, we are exposed to them, we do understand them, just coming in and helping them understand the landscape that they're working in. Because a lot of companies don't need you. You may not be surprised, but they don't even they don't even dive that deep to really understand the landscape that they're working in the breadth of it. Supply chain, right, just just as one area, I'm just giving you one air supply chain, they don't really understand the depth of their supply chain. If we're talking about the federal government, we're talking about the DIB defense, industrial base, tons 1000s. And 1000s of companies are part of that supply chain. Really understanding the details of that supply chain? Where are they getting those? Where are they getting those parts from? Where are they getting those components from? Are they getting them from a place that they're supposed to be doing business with? If we start talking about threats, are they getting them from a place they should be doing business with one thing that we know is that you know, our nation, state adversaries are incredibly sophisticated, right? They, they spend, they're very strategic, they spent years developing right their way into a certain environment, whether it's a certain type of business, certain type of government, they spend years developing that, and they study that in great length. And so they're looking for a way to get into that supply chain, and they know it better than we do better than our clients know it. So that's, that is our job getting in with them, and just helping them understand their environment, we can talk about all these complexities of all this new technology that's coming out. But really, the heart of the matter is understanding that operate, you know, the environment that you're operating in. In

Rodney Snyder - Guidehouse [7:10] fact, with supply chain, just to give you an example, most understand who their primary suppliers are, what they don't understand is the other suppliers that are deep inside the tiers of that supply chain. And so the very first step we take when it comes to supply chain risk management is understanding illuminating who's in the supply chain, again, not just at the first level, but at multiple tiers. And then it's really starting to develop, what's the risk involved, and all those different participants, those different entities, who else is touching what third parties are touching our system or network, and really start then really starting to look at what are the mitigation opportunities we have. And finally, how do we do continuous monitoring to make sure it's not just a one and done, but this is something continuous. And we're seeing this as critically important in the physical supply chain, and even increasingly evermore in the cyber, and in the software coding part of the supply chain. So that's just one example. But on cyber, it's the exact same issue, you have to understand everything within your environment, to then be able to assess it and take measures

Patrick McArdle - Guidehouse [8:15] to build off Ronnie's you know, statement there about, about the supply chain and getting to know your customers. It's also helping you know, our clients understand the expectations of the federal government, it's not just knowing your customer is sometimes you are expected to know your customers customer and look further down that line, there is that expectation of government and you need to help them understand.

Tom [8:36] And so in thinking about all of this when you bring this to companies than I imagined, and you can tell me the message also is this is not just something you throw over to the compliance department and let them worry about right? Absolutely.

Marianne Bailey - Guidehouse [8:49] Compliance is like to me as a cyber person compliance is like step one, you want to be compliant, but it's well beyond that. And that's one of the things when we talk to them that they really don't understand a lot of times they don't understand the risks. They could be in a critical infrastructure environment, right, that is very near and dear to the heart of the United States of America. And they might not understand why some other bad guy would want to do something to take them out. And and we haven't talked about bad guys, but you know, we are talking about geopolitical. So it's not just nation state. It's also criminal activity. It's terrorist activity. Right? And it's just your average every day run of the mill criminal, you have all these different bad guys that you have to, you know, protect yourself against, and they're not looking at it from the lens that they would be a target for somebody for a specific reason. Sure. You

Patrick McArdle - Guidehouse [9:42] definitely need more than just the compliance department. Right. So the whole enterprise needs to operate as a single unit so great. The compliance department has recommended a new software be brought in to help us prevent x y&z Well, if the technology team that's implementing that doesn't have a good grasp of what that technology is actually To intended to capture, it may not be set up in the way that it was intended. And so that's why you need to have, you know, fully full integration, right of all the all the parts of your enterprise operating as one in order for there to be a good shielded defense.

Tom [10:13] And that's a good point, you make two geo political means geo right here in the US have a is a source of threats.

Rodney Snyder - Guidehouse [10:20] So that's where it starts. But again, everything we're talking about emanates out across the globe. And that's why these issues about it being so much more than just being in sort of that defensive compliance, check the box mode, it is about being proactive, taking a sort of steps, looking at not just individual pieces of this puzzle, whether it's sanctions, or whether it's fraud, and preventing that or whether it's the cyber domain and how it's growing. But it's really going out and making sure that you're understanding the environment, the government and the regulatory requirements has passed talking about not just your but abroad, so that you can really then sort of, again, make that cascade out across the world. Alright,

Tom [11:00] we're gonna get into cyber fraud and sanctions. But first, we're going to take a short break, I guess today are Patrick McArdle, Maryanne Bailey and Rodney Schneider. They are all partners at guidehouse. I'm Tom Tim. And this is the evolving complexity series growing proliferation of geopolitical risks, threats and security vulnerabilities sponsored by guidehouse here on Federal News Network. My guest today are Patrick McArdle, Marianne Bailey, and Rodney Schneider, all partners at guidehouse. I'm Tom Temin. And let's go into some of the details that we were talking about earlier in some of these geopolitical risks. And I think probably top of everybody's mind these days, and for some time now is cyber, the cybersecurity risk, but cyber, even beyond cybersecurity, the cyber supply chain, you know, as you mentioned earlier, so what are some of the particulars here? What do people need to specifically worry about in the here and now, that's different from a year ago, and five years ago?

Marianne Bailey - Guidehouse [11:58] I think people just need to really be more conscious about their environment. And we talked a little bit about that, anytime that we go into a client site to work with them. That's like the where we start, what is your environment? We talked about modern technology coming out and things like cloud, that doesn't give you a pass. I've I've had many, many clients say to me, we're okay, we're in the cloud. Well, great. You're in the cloud. Now, what are you doing on the cloud? Right? What's happening? How are you protecting your data? Sometimes it makes things more complicated, because things are much more dispersed. And they lose track of where their data is, who has access to their data, who's touching their environment. So all it becomes very complicated, because you have to know all of that stuff. You have to know who's in your environment, you have to know what they're touching. You talked about compliance earlier, you know, most companies that we've seen that were breached organizations, even government organizations, they were meeting their compliance, right. They weren't like dropping the ball on compliance. But that's just the beginning. And you have to do other things. We talk about things like it guidehouse multifactor, authentication, identity and access management, it's a huge deal for us. It's not a new thing. I mean, I've been working this almost since, you know, I started in cybersecurity, it's evolved a lot. We use it all the time as individuals, right. So you use it, when you bank on your phone, we all use it. It's gotten tremendous traction, because it is such an imperative. And that's like the building block for cyber. If you don't know who's on your network, if you don't know what they're doing, if you don't know what they're touching, if you don't know your devices, don't worry about the rest of the stuff because you've lost, you've lost it.[

Tom [13:36] Sure. So that gets into the observability of what's going on in your environment. And also your configurations, patch management, some of the basic hygiene, ZZ that are still a challenge for a lot of companies and organizations.

Rodney Snyder - Guidehouse [13:47] Well, and it goes even into things like strong passwords and changing those passwords. But it all ends up at a place that Marian in particular works all the time, which is zero trust architecture, and that sort of complete turn of how we look at the environment that we set up in terms of security and trust.

Patrick McArdle - Guidehouse [14:03] Yeah, and I mean, from a fraud aspect, we've seen, you know, considerable challenges with some of the new technology around AI and generative AI and sort of Marianne touched on some of the we have you have multi factor authentication, some people using voice authentication as second factor with generative AI, they've been able to capture your voice and then use that the backdoors have been able to use that to gain access to various accounts. So it's, so as much as technology has been enabler for for people that use it the correct way, there's also been an enabler for those that choose not to.

Marianne Bailey - Guidehouse [14:37] And that really is like cultural education, really, for our society. If you think about it, you're used to hearing somebody you recognize a voice, you know, they're inflections. You trust it, right? This is kind of a new thing for us. Well, guess what? With AI, they can sit here and you have lots of voice out there, they can you know, capture that and they can make money, they can make a voice script that says anything. They wanted to say if you're a person of authority somewhere in a company, right, you should call somebody say something, they're going to do something. The reason cyber has become so complex, because it touches everything. And we'll talk about that with fraud. People don't break into a network just to break into a network, there's some end game they want. If we're talking about geopolitical things, and we're talking about nation states, it could be right to steal secrets, it could be intellectual property, they want to put your company out of business, we have examples of all of that stuff. So we've seen all of it. It's not like far fetched and far reaching. So it's something they want to do.

But now everything is digital. Everything that we're doing is digital. So it's out there on a network that's out there and environment. Bad guys can get it, they can have access to it. And so one of the things that we talked about very specifically is resilience. How do you how do you establish your environment so that you end up with a resilient environment, your businesses resilient, your government agencies resilient? What are you doing? How fast can you catch a bad guy in your network? How quickly? Can you turn it off? How do you segment them? And keep them you know, only in a certain part of your environment? Before you catch them and get rid of them? And then how fast can you kind of reconstitute your environment. That's why cyber has gotten so complex because it impacts so many things. And

Tom [16:24] I wanted to touch on fraud too. Because I mean, every day there's a Brit, it heartbreaking story coming out from one agency or another and all of this pandemic spending and disaster spending, infrastructure spending, talking hundreds of billions at a time, you know, real money going out through fraudulent means. And and companies have the same issue insiders, or external parties who say somebody in authority mimicking the voice and all of a sudden money goes out. So what are some of the trends now? And how do you help people mitigate the proliferation of fraud threats?

Patrick McArdle - Guidehouse [16:59] Yeah, so that, you know, as I just touched on, that has been the sort of latest the infusion of AI generated responses to multi factor authentication, you know, has been a has become or is a problem facing many institutions, especially financial institutions who were using voice as a second factor authentication. So that's been a big challenge. We talked about, you know, geopolitical, we talked about companies, companies, or companies are no longer just based in a single, you know, country. So I have some part of my operation, you know, offshore for, you know, efficiency reasons. And what that does is, you're now in another region, another geopolitical region, what are the safety and security standards? They are, are they the same as those in United States. So sometimes there's some of there can be some ignorance right on on the US companies parts, they believe that, hey, whatever we do here in the US, that's the same as it is in every other location, it may not be. And that's a challenge that you have to face, especially if you outsource some of that you need to confirm what the security vulnerabilities are in those countries. Because they may not be the same as those where you're where you're based. Because

Tom [18:14] AI can also work against fraud to have deployed in the right way. And you can screen applications and incoming requests, and whatever it is that your context brings you. Right, anything

Marianne Bailey - Guidehouse [18:26] with patterns, anything with automation helps you right, but but, you know, the bad guy has those same tools to use to their benefit, too. So we just have to be smart about it,

Patrick McArdle - Guidehouse [18:36] ya know, we have we have, you know, been working with a number of clients implementing sort of machine learning around some of their historical fraud patterns, right. So incorporating what the historical fraud patterns, developing algorithms that can help you identify those in a more efficient manner, therefore giving the investigators more time to focus on certain vulnerabilities, right, so you can risk rank them based on this machine learning? Right. So that said, I spend more time on higher risk situations and less time on lower risk situations, because there is always there's only a finite amount of funds to to address this in many cases, so you're trying to be as effective and efficient as possible.

Tom [19:19] They used to say that a accountant stealing could never take a vacation, but maybe with AI they

Patrick McArdle - Guidehouse [19:47] no, it sanctions is a huge problem again, it's our government trying to or imposing its political views or It's protecting national security. So as a result that imposes sanctions. And one that's very common for everyone is economic sanctions. And that potentially forbids transactions with a particular person, country or business. And you need to make sure throughout your geopolitical supply chain, right, so that that you are addressing those. So the again, we got back to sort of the customers customer, the first person I may be dealing with may not be sanctioned, but the person, the company that they're dealing with, potentially is, and that's something that you need to be aware of. And, you know, again, if you're a US business, doesn't matter whether you're just operating in the US whether you're operating outside the US, you have to comply with those sanctions, right.

Tom [20:42] So you may have the best intentions and not deal with any primary supplier that is in a sanctioned area. But as you mentioned earlier, if you don't have visibility down those tiers of your supply chain, doesn't matter what your intentions were. And

Rodney Snyder - Guidehouse [20:57] it keeps extending sanctions. Many people think that it's about sort of the big frontline headline grabbing countries in the world. But it's about so much more. For example, recently, Russia was sanctioned, because infected is pulling miners out of Ukraine, and forcing them into Russia to be educated, indoctrinated. Another example is in China. China's been sanctioned recently with respect to Tibetans, and the Uyghurs. And so the, the extension of sanctions continues. And this is what I mean by geopolitical extended out into other parts of the world, and well beyond sort of just the wartime situation, or something like terrorism or drugs, which is what so many people think about, because that traditionally has been the case, these things continue to evolve. And it's very important for the primary companies or agencies, but also to know who else was in the supply chain, that that impacts.

Marianne Bailey - Guidehouse [21:55] All right, final word. Now, we're just gonna say, so we talked about these geopolitical risks and threats, because these things are all interconnected, right? We can issue sanctions on a country, this, we've seen this, there, immediately, we get a cyber attack a massive cyber attack to the United States, right? Broad, obviously, in cyber are very, very interconnected. Because we talk about things like synthetic identities, which is a big deal on how you steal information, how you steal data, how you steal bank accounts, all that kind of stuff. So there's this huge connection between what's happening globally. You know, what's happening at home, and then all these other areas that are impacted by it. All

Tom [22:29] right, so you can't leave any stone unturned and make sure you understand your supply chain, really in depth, I think seems to be the takeaway here today. All right. Well, thank you very much. My guests are Patrick McArdle, Maryann Bailey and Rodney Schneider. They are all partners at guidehouse I'm Tom Temin. You're listening to Federal News Network. For more on this discussion, please visit Federal News network.com and search guidehouse

Transcribed by https://otter.ai

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 17,000 professionals in over 55 locations globally. Guidehouse is led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit guidehouse.com.

guidehouse.com

@guidehouse

linkedin.com/company/guidehouse

outwit complexity™