Resilient: Confronting the COVID-19 crisis

Actionable insights to help businesses respond and recover

Episode 24: Critical infrastructure risk: Creating a secure and resilient world

Host:

Mike Kearney, partner and chief marketing officer, Deloitte Risk & Financial Advisory

Guest:

Robert (Bob) Kolasky, assistant director, Cybersecurity and Infrastructure Security Agency's National Risk Management Center, Department of Homeland Security

---

Mike Kearney: Welcome to Resilient. My name is Mike Kearney, the Risk & Financial Advisory CMO. We have completed over 20 episodes in our Confronting the COVID-19 Crisis series. And what's crazy is that there's so many topics that we still need to cover related to the ongoing challenges of the pandemic and opportunities that are being presented on a daily basis. I have to say that is why I love the Resilient series.

Today, we are going to ask questions about risks to the nation's infrastructure. How do we build trust, resiliency, and security in a complex and interconnected world? How resilient is our nation's critical infrastructure? What risks are emerging? Are our public and private risk mitigation strategies to combat the threats keeping pace? And who is leading that effort to manage these risks?

Bob Kolasky is who is helping keep us safe. Bob is the director of the National Risk Management Center (NRMC), which ultimately resides under the Department of Homeland Security. He brings a unique perspective, especially on how the crisis has impacted the 16 critical infrastructure sectors and the 55 national critical functions. The NRMC is really at the intersection of government and industry, and this is really important—it advises businesses, industry, and the government on how to best secure, protect, and keep resilient those functions that are so vital that their disruption would have a debilitating impact on the economy and our national safety. Let's hear what he has to say.

So, Bob, you are the man that sees risk everywhere, obviously in everything you do. But one of the things that we've heard, especially through many of our recent Resilient interviews, is that hope is really what makes people resilient. So, what hope do you have for the future?

Bob Kolasky: That's a good question. I like the way you frame it. I get asked a lot sort of, "What's the thing that keeps you up at night?" And I always resist that question. I'm sort of, the way I like to phrase it, "What's the thing that gets me out of bed in the morning?" And I think that's really what we're talking about. What gets us out of bed in the morning here is that, my hope is that we have a number of smart people, we have a lot of committed partners across the industry and the government, we have a lot of innovation out there to go at the big problems facing the nation. You find hope in people. You find hope in the willingness to look hard at who we want to be as a nation, understand what's the risk to that, and then get after the problem.

Mike Kearney: You know what? I love about that answer! And I do ask this in different forms in every interview, I do. It's oftentimes about a circumstance in the future or something that an organization is doing, but you've cut it back to, I think, which is actually the most important thing to our future, and really every industry, every sector, every issue we face. And ultimately it comes down to, if you've got good people that are committed to do the right thing, things will end up in a good place. So, I love that, that you actually focused on kind of the people aspect of it.

Bob, I want to ask you just kind of to set the table, what is the focus, because it's going to be a term that many people haven't heard, but what is the focus of the Cybersecurity and Infrastructure Security Agency (CISA), which is kind of a mouthful? So, what is the focus?

Bob Kolasky: Sure. So, the bureaucratic answer is we are the agency that's responsible for securing federal networks and working with critical infrastructure partners around the country to make sure that critical infrastructure, energy, banking, and finance, et cetera, are up and running. And so, the Cybersecurity and Infrastructure Security Agency really is in support of the nation's critical infrastructure and our federal networks. But we have a couple of pithy ways that we describe what we're doing. One of which is, we serve as the nation's risk advisor. We are out there, and we're going to talk a lot about risk, but we are out there trying to understand risk and get information on how to reduce it into the hands of security professionals, in the hands of planners, in the hands of financial professionals, so that they can do something to reduce risks. So, we play a key advisory role.

And then the other pithy way we describe it is, we want to help defend today and secure tomorrow. We want to help, on the defend today, we want to be ready if anything happens today to be able to close vulnerabilities, anticipate threats, but we also then want to build toward a more secure tomorrow. As we do things like as a nation and as a globe, build out 5G networks. How can we make sure that's done securely and we can take advantage of all the increase in bandwidth and connectivity that's going to come with 5G and not be sitting back 10 years from now saying, "Oh shoot, we didn't think about the ways that our adversaries might hit those networks." So, we want to be focused both on what we have to do today, but also think about tomorrow.

Mike Kearney: And then there's this National Risk Management Center. So how does that connect with the Cybersecurity and Infrastructure Security Agency, if you could just touch on that as well?

Bob Kolasky: Sure. So, I run the National Risk Management Center within CISA. I'm one of the CISA assistant directors and, going back to the pithy ways, we really help develop the analysis to give the risk advice that is in CISA goals. And we really are focused on, particularly, on the secure tomorrow aspect of CISA's mission. The National Risk Management Center is a planning and analysis and collaboration center. It's a place that has the best information out there on how critical infrastructure works and risks to critical infrastructure. And we are capable of doing analysis in the face of whatever incidents or threats we're facing to understand how those threats turn into risk and could propagate in the system. But it's more than the analysis, it's in the planning and the collaboration, it's bringing industry and government together to do something about those risks, whether it is to secure 5G networks, whether it is to secure our elections. We're doing a lot of work around information, communications, technology, supply chain security. We're thinking about how you secure the GPS system, the position navigation timing long term. So, when we see things that are kind of strategic risks to the nation's infrastructure, we put together the plans, we bring together the people to do something about the analysis to reduce risk.

Mike Kearney: It sounds like actually a really cool role. What led you to this role as the associate director of the NRMC?

Bob Kolasky: Patience and endurance. So, I've been with the Department of Homeland Security about 15 years doing risk and preparedness and infrastructure work. My first most significant job in the department was really defining how the department approached risk management. And I wrote a lot of the foundational documents there. My background previously with the department, I was a consultant. I did time as a journalist. I have a master's in public policy, where I focused on particularly business and government policy, and economics. And so, it's a good background, I think, into this. When [DHS] then-secretary [Kirstjen] Nielsen established the National Risk Management Center, she was, I think, in selecting me, looking for somebody who understood the fundamentals of risk, had good experience working with industry, and enough experience to drive it really into action. And for me it's a good combination of my experience and academic background. And I don't know, I think I'm a natural risk thinker in some ways. I like thinking about the world in sort of organized frameworks.

Mike Kearney: What's fascinating about it is your background in journalism, because one of the things that I find in the work that I do with a lot of risk leaders, mostly at public companies and things of that nature, is the risk management professionals need to communicate effectively with people who aren't in risk because they see the world very differently. Do you think that journalism background has enabled you to do that because I've never, quite frankly, that is not a common background, a journalism background, but now you're in risk, which I think is fascinating.

Bob Kolasky: Yeah. So, what I found as a journalist is often, and I was writing for one of the early internet publications, and you had to quickly understand an issue and translate that issue to readers, for the purpose of readers. And so you get on the phone and you learn, you do the reporting, but you're constantly learning something new, and in some ways, as a journalist, you're dealing with a little bit of uncertainty because you're never an expert, unless you have the luxury of writing on one thing, you're not the expert at what you're writing on, you're talking to the experts and you're trying to translate the experts' opinions into something that resonates with the reader. I mean, if you think about that from sort of a risk perspective, what we're trying to do, and all the subjects I just brought up, I'm not an expert in how elections work, I'm not an expert in what a 5G network looks like. Talking to the experts, bounding the technical knowledge, recognizing that there's uncertainty, putting barriers around the uncertainty, and then thinking about what recommendations are going to resonate for the audience, whether it's a policymaker, it's an operator, it's somebody who's making financial investments. So yeah, I think it served me well as a background.

Mike Kearney: So maybe talk a bit more about the NRMC and what areas it specifically has responsibility in overseeing, especially in critical infrastructure protection, which obviously is your mission. So, if you could just share a bit about that?

Bob Kolasky: Sure. We define the key things around what our critical infrastructure risk is and maintain sort of that definition. So last April, we published a list of 55 national critical functions that are the things that are so important to the nation's economy, national security, community wellbeing, that they need to be able to function for the country to be healthy. And the reason you define functions is then you think about risks, about things that could cause loss of function. And so, defining the risk and then within that, we also sort of manage the understanding of what is most critical, which companies are most critical to those functions, which geographic assets and facilities are most critical, whether it's an electricity substation or telecommunications hotel, or something like that.

And so, we have this lay down conceptually down to the hard asset of "these are the things that are most critical from a national security perspective." And we put that information together. And a lot of our work is the modeling, the information gathering, the technical analysis, and then the visualization in support of how to lay down knowing what is most critical. And then we apply that knowledge to strategic risk challenges, operational risk challenges that are facing the homeland. So, having that rich understanding and then using it, so we'll talk a little bit about COVID, what's the most critical infrastructure that needs to be working for the country's recovery in response to the pandemic. The underlying knowledge allows us to do that and then prioritize within that. So, a lot of our work is around that area, but then we also do work where something has been deemed to be a national priority and we need to manage the risk to it. We lead the department's efforts to support state election officials in securing elections. The president last year declared emergency in the nation's information communications technology supply chain, and the fact that we're seeing threats from China and other places, and we helped put together the plans to address that emergency.

Mike Kearney: Can you just give some examples of some of those 55 different functions?

Bob Kolasky: Yeah. So, the functions include things like transport goods and materials via air, transport goods and materials via rail. So, transportation functions, communications functions, operate core networks, be able to communicate wirelessly, IT functions, including things like identity management and intellectual property development. And then, banking and finance, maintain a liquidity system; energy, having the ability to generate and transmit electricity; extract fuel. So, it's functions like that that allow us ultimately to create the end state that the lights are on and we're communicating with each other and we can move things around. We can operate a health care network. There are a number of functions that are related to health care networks. And it's a good way of framing, again, the things that have to work, and I know we get it right if I can look at the list and say, "If that thing's not working, that's going to be a bad day for national leadership. And they're going to be meetings all over town and everyone's going to be killing themselves to get that thing up and running." And so that's a national critical function.

Mike Kearney: And it also sounded like what you do is you ultimately identify those functions. You reconcile it down to, "Okay, now in that ecosystem, what are the critical companies and then what are the risks?" But it sounds like you, and you said this up front, but you have an advisory role. So then how do you ultimately work with those end companies in elevating those risks, sharing the data. It's almost like you're a consultant working for the government, going out to these companies, and you really probably need to collaborate with them and help them understand why these risks are so important. But can you talk a bit about how you ultimately advise these companies and what you do and how you get their mind around these things?

Bob Kolasky: So, I like to use tangible examples, and I'll use tangible examples of the things we're actually doing. So, one national critical function is the availability of position navigation and timing (PNT) services. A lot of that comes through global positioning, GPS, through satellites and things on your device. But a lot of critical infrastructure depends on precision, position, navigation, timing. And, so that's a function—we have through sort of legislative mandate and executive mandate, recognize that there's significant risk and we probably don't have as resilient position navigation timing services as we need. You can trace some threat activity from other nation states, maybe that's a way they may look to hit the United States or sort of the global order on that. And so, let's start, let's talk risk language. PNT is a critical function and we believe there are strategic risks. So, we need to figure out how to make that system more resilient.

In this case, the work starts—and we're talking businesses—we do a lot of work with sort of the receiver companies and the underlying suppliers of PNT. We help sort of encourage them to address vulnerabilities in their PNT receivers, give them information about where we see the risks that will lead receivers to be harder coded and less likely to be attacked, but that's not the only way you manage risk here, receivers, perhaps, your underlying concern is sort of single point of failure of the actual signal coming from a satellite or things like that. We've done a lot of work evaluating backup capabilities for PNT and, there's policy work, R&D investment, and other incentives to establish a more rich, market-based backup capability.

And then the end users of PNT, we're working with them to encourage them to understand their sources of PNT, to understand what would happen if there's failure and the availability to that, to do planning around failure options, and to perhaps make investments in backup capabilities. So again, if the risk of failure is too high for their businesses.

And so, you see in there, I think, a pretty good mix of how we generally work with industry. Get information out, encourage them to do more, to be more secure and more resilient based on that information. And if that information is not good enough, if that encouragement is not pushing them to make business decisions, we try to come up with investing in innovation that might change the cost end of some of those business decisions or incentives to encourage them to reduce risk. And so, it's a mix of that. I find businesses generally don't want to take too much risk to their core business functions. And if their core business functions matter to national security, we're going to encourage them to do what naturally makes sense for them to take less risk. They might not have the financial wherewithal or the financial incentive to go all the way there. And that's where we look for sort of some innovative solutions to help push them to allow them to do that.

Mike Kearney: Is there anything that you've picked up through this process, because ultimately there is kind of the art of persuasion, although as you indicated, these are really important assets. And so for them not to listen to you guys probably wouldn't be a great strategy, but my guess is from time to time, they're like, "I get what you're saying, but this isn't a priority for us at this point in time." Is there anything that you would recommend, because we've got a lot of risk leaders that listen to the podcast, around how do you persuade another party to make these investments in risks, and how do you do it in a way that resonates with them? I'm guessing that's probably come up from time to time.

Bob Kolasky: I've found that you start by sort of a continuing relationship of trust and building trust. That's not, there's nothing profound in trust, but you have to meet industry where they are, understand sort of what drives a business decision, recognize that some of the time—recognize that they're trying to get—do the right thing in their business contexts, but it doesn't always get you there. And so, you talk, I'd like to as much as possible talk in terms, in business terms and what makes sense. There are things that the government does that frustrate businesses in terms of multiple government agencies working on the same problem, lack of harmonization of regulation, inefficient regulation. And if we can address some of those issues and lower the costs of a business, if there's less compliance costs, they can put some of that cost into security solutions. My persuasion is, first of all, assume people are trying to do the right thing and want to do the right thing, but they're bound by their constraints in their knowledge and try to get to a place where the decisions work within their constraints.

Mike Kearney: Just thinking about some real-life examples, you've already kind of touched on some—COVID, 5G, state elections. What are some of the biggest risks that you see out there right now that you guys are focusing on?

Bob Kolasky: Sure. So, first and foremost, the pandemic and the 2020 elections are top of mind right now for where our energy is in CISA and National Risk Management Center. The 2020 elections are obviously going to be a really important to where we are as a democracy. But in the middle of that, we don't want our adversaries to take advantage of the fundamental things going on and give less confidence in the results of the elections. We saw in 2016, in a lot of different ways, attacked the integrity of our democratic processes. We want to be on the alert, and we are on the alert to make sure that doesn't happen again, that other adversaries don't follow the playbook and that the voters have confidence that their votes and their intended votes are secure and will be counted accurately and that we will have an accurate election.

So, we have within CISA just a ton of energy around looking for anything that could undermine our democracy. At the same time, and that sort of overlays with the pandemic, at the same time, again, we are in the middle of, we saw the GDP numbers today, right? We're in the middle of time, whether we want to talk about this from an economic perspective or loss of life perspective, an illness perspective, or community wellbeing perspective, and that stress would be exacerbated if our infrastructure wasn't working. If key critical functions, those functions are all necessary for response and recovery. And the pandemic's not a first order infrastructure crisis, but if infrastructure doesn't function, we're not going to bounce back from this as quickly in communities. People, individuals, are going to be in worse shape. And so, again, looking at the infrastructure, working with industry to make sure essential workers can work and commodities are being delivered. And the economic conditions are such that power and water, and banking and finance systems keep working. So that's a lot of my focus right now. And on top of that, again, are sort of things that other governments might look to do or adversaries might look to do to take advantage of some of the current stress we're dealing with as a country.

Mike Kearney: Can you talk a bit about I guess the interdependencies that exist between public and private industries and how you work with them? Because obviously, many of the most important organizations that manage our infrastructure, are private organizations. Could you talk about kind of those interdependencies?

Bob Kolasky: Yeah, sure. So, let's use power and communications companies. Whether it's electricity providers, communications companies, both of those are run by, largely put together by the private sector with federal investment in creating those networks and some order of federal and state requirements to deliver a level of resilience and delivery. And so, from the get-go power utilities, communications companies can't work without government policy enabling them, and so these are while privately run, it has been federal/state policy that have enabled these systems to work strongly. So, we are interdependent with each other. And so, when you talk about, let's go with the power companies. When you talk about the power grid and cybersecurity becomes more important, we have to have an information sharing structure where we let the power companies know what we know and that they can then build in practices to help secure the grid. We invest as the federal government in innovation that can then just be operationalized by the utilities themselves. We share information with them. We collect intelligence to understand if things are going to be attacked. We work with them to sort of scan and understand vulnerabilities to the system. And then, there's this level of state and local government where some of that cost costs utilities more money, which means they're spending more money to deliver power. The consumer is going to ultimately have to bear some of the costs for that investment in resilience. And you've got to work with the public utility commissions to make sure that the cost is accurately passed on to the consumers. So, it is a fully interdependent relationship. The good thing we've been able to do over the last 15 years that we lean on at CISA is we've set up the structure where CISA and the Department of Energy work closely with the utilities and state governments to put together these plans, have these strategy conversations, talk about vulnerabilities collectively. We work together. I have the opportunity to sit with CEOs of a lot of the major public utilities along with the Department of Energy and talk through all of this stuff and hear from them what's going to help them build a more resilient and cyber secure grid, and work through that process together, and it becomes a partnership, it becomes a running conversation. And going back to where it started, I think that's what we've got to have. At this point, if our adversaries are going to attack our power system, our power system is part of our national security. And we have to bring those utilities into our national security dialogue and get them the information tools they need to protect themselves against a foreign government.

Mike Kearney: So, Bob, one of the things you talked about, which I find fascinating, is being in these meetings, sitting down with some of these CEOs and talking to them about the risks of potential decisions that they're making that are risks to their infrastructure. One of the things that I think is critical, and I'd love to get your thoughts on this, is the risks associated with certain strategic decisions that these CEOs make, and obviously there are downstream impacts potentially to our infrastructure. Do you ever give guidance in how CEOs and other leaders, especially in the private sector, should think about those risks when they are thinking through strategies? And I'm really interested in this because I've spent a lot of time in strategic risk over the last several years. And what we oftentimes find is some of the biggest and most important risks that an organization faces is because of the choices that they make and their strategy and the choices that they don't. So, if you could touch on that, that would be fantastic.

Bob Kolasky: Yeah. So, let me give you a tangible example of something that we're studying right now. And we're doing it with industry and government working together. But related to the pandemic, you saw that availability of certain commodities was stressed and not certain because maybe where the manufacturing is done, and it's done somewhere around the world, there's a lot of manufacturing going on in Asia, for example. And they become sort of single points of failure. If you can't get something from Asia to the US, perhaps you can't do something from a business perspective. And of course the decisions, Deloitte knows this well, you folks know it well, of course there've been business decisions along the way to manufacture things where it's cheapest or to not have redundant manufacturing capability, redundant sourcing, things like that, and do more just-in-time delivery and all of that. And ultimately that's created a less resilient supply chain for commodities. And if you lose trust in where things are manufactured, for whatever reason, it could also create a less secure supply chain.

And so, economic drivers, market drivers, business factors have been the reason that a lot of those decisions were made. Now's a moment, and I think companies recognized that either they were stressed or they were close enough to being stressed in the middle of the pandemic that maybe they had baked out too much resilience or they were too lean. And so, I think there's a willingness by industry, and so we're starting this now, we're actually using a public-private taskforce that I co-chair to do a study. There's a willingness from industry to be maybe a little bit less lean in their supply chains or think about tightening their supply—shortening their supply chains, their value chains around that. And there's government-industry conversation about, if you're going to do that, how do you do it in a way that's going to leave us functioning in the strongest way, and what can the government do to help encourage that to happen? And what are the factors that make it less likely to happen? And can we remove some of the barriers? And so, yeah, we're giving advice in that area, we're listening, and ultimately we hopefully will be in the business of reducing some of the barriers to more effectively and efficiently build stronger supply chains, logistics chain.

Mike Kearney: I love that example because obviously I have a lot of clients that have actually dealt with that over the last four or five months. I'm curious, is there anything—any tangible examples of a tool or a process or a way to kind of assess those risks that you've seen? And one that we are seeing a lot more interest from our clients, and we've been talking to them about it for years, but it's really catching on now is scenario planning so that you could begin to see, because of these uncertainties, how could some of these scenarios play out, which is

a good way to identify using your supply chain. I mean, if the organization did robust scenario planning, they potentially could have seen a future where their supply chains were constrained. Are there any other tools or things that you guys are looking at that, if you're listening to this, that you'd recommend a risk leader potentially adopt or look at?

Bob Kolasky: Yeah. I mean, a lot of it is still tools around illumination and pulling out data and getting deeper into sort of understanding how the complex chains work. And so, a lot of our conversations start with encouraging "we're doing this for our own purposes," encouraging a better understanding of what is the most valuable thing in your system and some ability to evaluate that. And then how that valuable thing's produced and illuminating that and taking advantage of what's known and what can be gleaned from that, what's important within the illumination to make trust judgments. And so, I think there's a lot there. And then as part of making trust judgments or confidence judgments, setting up metrics to evaluate. But I'm pretty bullish on the evolution of our ability to understand complex systems and pull data real time to test how those complex systems are working. What I really want to do at a National Risk Management Center is bring some of that innovation that I think is largely going on outside of government, bring that within government and take advantage of that system and scale it so it's easier to do.

Mike Kearney: Well, you just touched on one of the biggest issues my clients quite frankly had. And that was how do you get data real time when these risks are unfolding or these crises are unfolding? Just simple things like, "Where do our employees live?" "What devices do they have?" I mean, just simple things like that. My clients struggled with that. Not that they didn't have the information or the data, it just wasn't available real time or in a manner that allowed them to consume it so that they could make better decision making. So, I love the fact that you've touched on that.

Bob Kolasky: Yeah. I mean, you can't be a Homeland Security person without recommending planning, and testing and exercising. Some of this is simple, but it's like, I mean, you're talking about scenario planning, but go down from scenario planning, which is sort of alternative world planning and also into scenarios that you're most concerned about. Go through that and really go through the discipline of testing whether you've got a plan in place to deal with that scenario, whether you can pull information. A pandemic was wholly in the realm of something that should be in—people who have the ability to make an investment in continuity planning—it should have been in continuity plans. I hope it was in continuity plans. It should be tested from time to time. And I think one of the things we did see, and I assume you saw this with a lot of your clients, a lot of global businesses had thought through the pandemic scenario. Obviously any one scenario, COVID is different than the pandemic maybe you planned against but have thought through having to do business. And I think it has served us well.

Mike Kearney: Yeah. One of the things I think took my clients by surprise wasn't necessarily the pandemic, because I think we all knew that it potentially was going to happen. It was shutting down the economy and essentially having every one of your workers, especially in areas that traditionally had not been able to do things virtually, now they have to, oh, and by the way, we have to do this within 48 hours. I think that was the black swan, if you will, that my clients didn't necessarily plan for.

Bob Kolasky: It's interesting—it's the policy interventions on top of the pandemic that guided all of this and that goes back to sort of public and private and doing it together. If we're in the same room having this conversation. And I've been in this room with a lot of different industry at different stages, "Here's what the government's going to do in response to this happening." And if you're not planning for what the government's going to do in response to what's happening, then you're not planning for what's happening, right?

Mike Kearney: Exactly. And, I'm just curious, did the crisis and COVID and everything that's happened over the last four or five months, has it changed how you look at the critical infrastructure risk environment? I know that you think about this a lot. So, my guess is you've probably had done a lot of thinking, but has the crisis changed any of your thinking?

Bob Kolasky: If you're not paying attention, all crises should change your thinking a little bit. I think planning for catastrophe, planning for high-consequence events, low-probability events, and bringing that into operations is something that the closer you are to something happening, you want to make sure that that continues to happen. So that's one area.

In terms of critical infrastructure, it gives you sort of a new understanding of sources of what's really important from an infrastructure perspective. I think for obvious reasons, public health infrastructure perhaps needs to be a bigger priority coming out of this. We talked a little bit about some of the supply chain things that think a little bit differently with it. I think it's been pretty impressive to see kind of the communications and IT underlying infrastructure surge to meet the change in the way we're all working or a lot of us are working, and the way communities are interacting. And that's an area where early on, we anticipated it being a significant source of risk and perhaps problems. And I feel pretty good about how our core infrastructure has functioned.

Mike Kearney: What about, what is your advice to leaders on low-likelihood, higher-consequence risk? You touched on that. What advice, and part of the thing that always fascinates me is you can do a lot of planning, but oftentimes you don't know what the next low-probability, high-impact risk is. What's your thoughts on that? What are you telling leaders?

Bob Kolasky: It comes down to leaving space for some thinking and investment in making sure—and I hope I will never have the opportunity, I won't make this mistake, or we'll learn this lesson—that

you've always got to reserve some level investment to think about the worst case to your function, if you're really interested in creating a resilient organization. And so carving out some of that, and I use carve out intentionally because if you don't carve it out, it just gets slowly merged back into thinking that normal operations and just doing a basic risk calculation on a day-to-day basis. So, you've got to allow for some space for that and testing the thinking in there. And so, a lot of it is really about making the investment around these things and stress testing. And picking some version of representative scenarios of the things that are really risky for your business and making sure you stress test it annually, whatever the scenario. And so, and then part of investment is then you might have to have a little bit of excess capacity in different areas, you might have to have things that over a 10-year period, you don't extract any value out of it. And how do you build that into your books? But you've got to think about that.

Mike Kearney: Yeah. I'd say one of the silver linings of the pandemic is that the next time a leader says, "Oh, that will never happen," you have this basis to say, "Well, actually something like that did." And I do think another thing that I would add to your response is, even having—creating the space and time to have substantive conversations with leaders. Because obviously you can put together the greatest analysis in the world, but if they're not looking at it, taking it seriously, and if it's not impacting decisions they make, obviously, it's not going to make the impact.

Bob Kolasky: I think the process is really important and the connection between the people who are doing this thinking and the leader, the board, the C-suite, whatever. I go back to some of what we saw—to social media companies in 2016 and some of what we saw in terms of adversaries using social media as an attack. And it wasn't that there weren't people in the social media companies that didn't see this as a possibility. It's that that risk maybe didn't get the attention it needed at the highest level. And almost anything that ever happens, there's an example of somebody somewhere in the bowels of government or in an organization, it's like, "Yeah, I've been telling you about that forever," but how does that, what's the process that gets that in front of the board and the C suite, make sure it gets the right consideration? This is risk governance. This is really thinking about enterprise risk management programs. And so I want to keep preaching the importance of doing that.

Mike Kearney: You mentioned 5G earlier—there's a tremendous amount of innovation in our world, which is great because that's how the economy grows and organizations thrive. But obviously that probably creates new risks. And can you talk maybe, especially from an infrastructure perspective and a cyber perspective, what are some of the implications of these new innovative approaches?

Bob Kolasky: Sure. So, I think a lot of what you're sort of asking about, Mike, is kind of disruption in the way services are delivered. If you want to get to the sort of simple technical level, we start to care a little more about software than hardware, that's what 5G is going on. We start to care a little bit more about data and how data flows to things. Things get more automated. It becomes a less analog-manual world. And so, let's just run with software, right? Software assurance, software security, software transparency, all of a sudden become a real high priority from a security perspective. And that's a whole new vector of how do you create software security. That's not the same thing as taking a device and hardening the device or isolating it. So, I think that's how we're trying to understand what are the major trends and they're all cliched at this point, AI and machine learning, smart automation and all that good stuff, internet of things, but that's all changing the fundamental way that infrastructure is going to operate in creating different exposures. One of the benefits of all that, I think, is more ability to on-the-fly isolate, so things cascade, and I think there's going to be real secure benefits of that if you can keep an attack from sort of being existential because you've created more diversity of the way things are automated. I think it's going to make security easier to do in some ways, but it's going to create new exposure and new vulnerabilities.

Mike Kearney: We talked a lot about the crisis that we've been going through. What can owners and operators of infrastructure do to better prepare for the next crisis? Meaning, and it may be things that we were talking about in advance of COVID, but maybe there's sort of some emerging things that they could do, but what are you recommending? And obviously that's a very broad question, but are there a few top things that owners and operators should be thinking about?

Bob Kolasky: Yeah, I mean 40 minutes or so into this, I don't know that I have a new answer to this. It is bringing risk thinking and security risk and resilience thinking into their enterprise risk processes so that it gets baked into conversations about where investments are going to be made in tradeoffs at the highest levels. I think that's a really important element of the whole thing. It is planning. It is exercising. It's testing. I mean, I'd like to see every board mandate exercises within critical infrastructure and certain exercises and then do something with the after action in its findings. I would be remiss if I didn't urge to set up public private—to set up partnerships with government where folks like us in the Cybersecurity Infrastructure Security Agency share information. You never want to meet your government partners who are going to help you deal with an incident the day of the incident. Make sure you've established relationships. We have a lot of programs that companies can take advantage of. So, make risk thinking part of your culture and bring it into tradeoffs, but do some investments in reducing risk.

Mike Kearney: So, Bob, I've got a final few questions. I call this my lightning round. What would you say is the top one or two qualities of a resilient leader?

Bob Kolasky: In some ways it's optimism, right? In some ways it is that you get in the middle of this and you've got a problem solving bent and you're optimistic that with attention, you can do something to make things better. And so, to me, resilience is fundamentally an optimistic concept. I think another aspect for a resilient leader, it's the ability to communicate and have trust. You

build up trust then you bank it and then you use it in the middle of a crisis. And it goes back to knowing people and everything.

Mike Kearney: I will say you gave the best answer—my favorite, maybe I shouldn't say best. My favorite answer to this question, I think I've now heard it, I don't know, 50 or 60 interviews, maybe from one or two people, and that is it's optimistic. Like you cannot, you cannot be resilient if you don't have hope for the future. I just don't think that those two things can live together because ultimately it is about leading your people. It's about making tough decisions. It's about doing difficult things. And if you don't have hope that there is a better world tomorrow, you can't be resilient in my opinion. So, thank you for that. And I probably just went over 30 seconds. What's the one thing, and you could take this at a very focused level, or if you want to take it at a higher level, is what's the one thing that you would change about how risk is managed? And I'm going to say, and it could be for owners and operators with infrastructure, but if you want to take it at a higher level, you can as well.

Bob Kolasky: I think it starts with not thinking about it as a quantification or a technical thing for how risk gets managed. Risk is a way of thinking and it's really ultimately about choosing the right mitigation strategies in the middle of uncertainty. And so I don't know if I would change—what I would change, but always focus on mitigation strategies in the face of uncertainty. Then you're using the analysis to narrow the uncertainty.

Mike Kearney: I love that because one of the things that I find, it's probably one of my number one recommendations to my clients, is oftentimes you get risk that is a separate, obviously separate function from the folks that are leading the organization. But the biggest challenge I oftentimes have is you got to make it consumable. And the leaders themselves have to have a risk mindset. It's not like something that you can delegate. And, quite frankly, that's oftentimes what we see in a lot of organizations is that it's not connected to the core decision-making of the business. And it's oftentimes something that the leader obviously takes into consideration but doesn't leverage or utilize the incredible assets that the risk management group may have. And so, it's simply about making better decisions with the information that is presented. So, I'd love that answer too. Okay, last question. What do you think is the greatest opportunity for the nation and/or our business leaders to become more resilient in the future?

Bob Kolasky: Ah, that's a good one. Let's go back and think about just being dedicated toward making the right investments, creating the right culture, and putting it in the right level of priorities. And so, that's where the opportunity is. Again, a lot of this is connecting risk and resilience thinking with strategy and financial thinking. And I think that's where there's opportunity.

Mike Kearney: I think that's a great place to end it because I could not agree more on that answer. Bob, thank you very much. This was fun. I always find these so educational, especially somebody that has dedicated his career and his life to risk management. So, I appreciate your time today.

Bob Kolasky: You're welcome. And thanks for having me. As you can tell, I enjoy these conversations, so I appreciate it.

Mike Kearney: Bob, wow, that was incredible. Thank you very much. I'll tell you, I learned a lot about the risks that really are out there that could impact what we all probably take for granted—our infrastructure.

We have covered a lot of topics over the last few months. And like I said at the beginning, we have a number of topics and guests that we're going to continue to bring to you. But I will say what's most important to me is hearing what you want to hear about. So, if there's any topics or guests that you would like us to bring on Resilient, hit me up on LinkedIn or Twitter. I've also been getting a lot of feedback, which is tremendously helpful as we continue to prioritize our backlog.

For more insights across all aspects of COVID-19, just go to deloitte.com on our COVID page. You can also listen to the Resilient podcast on Apple Podcast, SoundCloud, Stitcher, Google Play, and even Spotify. Until next time, stay safe and remain resilient.