TAG CYBER
LAW JOURNAL
NOVEMBER 2021

INTERVIEW: KRISTINA PODNAR / NATIVE TRUST CONSULTING

POLICIES TO TAME THE RISKS OF HYBRID WORK

A consultant explains why companies need to spell out the rules in writing.

***Kristina Podnar** calls herself a "digital policy consultant." She doesn't have formal training in tech (she earned an MBA in international business), but she learned the old-fashioned way. She worked at a startup in the early days of the web. It was a wild ride. "We did crazy things," she said. "We would upgrade websites without backing them up first." The result: a famous website was down for eight hours. On a Saturday. She survived to help companies navigate the digital world for two decades, most recently under the banner of Native Trust Consulting, LLC. Along the way she wrote a book called "The Power of Digital Policy." We thought she'd have a lot to say about our survey on hybrid work.*

***TAG Cyber:** What were some of the **findings of the survey** that seemed important to you, or were surprising in some way?*

Kristina Podnar: I found the majority of the answers predictable. Do folks actually have a cyber security strategy in place? The majority of folks said yes. Do they anticipate people continuing to work from home? The answer is yes. What I thought was really interesting was when we start to delve deeper into the results and look at things like how companies currently secure remote and hybrid worker connections. That was really telling. I was expecting things like MFA—multi-factor authentication—to be much higher than it was. And zero trust network access—I would have anticipated a much higher number. It's not so much the overarching results that were surprising, it's really getting under the covers, and getting to the substance that was surprising. And not necessarily in a good way. Because it points back to the need for additional awareness and better security practices.

***TAG Cyber:** Do you believe companies should establish policies and rules for employees when they are working remotely? And do these need to be written down and disseminated?*

Podnar: Absolutely. In fact, what I encourage the companies that I work with is not just to develop the policies, because it's really easy to create what I call shelfware. Shelfware is when I write down my policy, I put it in a really nice looking PDF on SharePoint, and nobody ever looks at it again. That's not going to get you anything. Save the paper. What you really need to do is write down the policy. If you're a small business, with maybe like 10–15 people, it doesn't have to be as formal. It can be written down on a napkin if you want. But yes, make sure that everybody's aware of what the policy is and practice it. You have to be very clear about the remote workers' responsibilities. You have to provide, in some instances, monitoring services. I'm a proponent of those—things like identity and access management control.

***TAG Cyber:** Should companies be monitoring their employees' behavior, and should they try to enforce the rules and policies they have established?*

Podnar: I think for a lot of folks, this seems like an over-the-top approach. But it is definitely something that we're progressively seeing in security measures for remote workers. Services can actively monitor that behavior and pick up any anomalies. And I think that that's actually a good thing. Because through data collection analysis, not just by manual review but increasingly through artificial intelligence, we can start to understand what is normal behavior, and we can identify, based on each individual user profile, anything out of the ordinary. This isn't meant to

threaten employees, as in, "If you go onto your Facebook account three times in a workday, I'm going to reprimand you." It is meant to monitor the fact that if I start to see you pinging Facebook 17 times a day, I know that something else might be happening. We might be experiencing a cyber event that I need to look into.

We have a situation with an organization that I've been supporting where an individual decided to take their laptop and go to India pre-pandemic. And that person was not supposed to be taking their laptop out of the country. They were very diligent, they were working every day logging on to every meeting. But at the end of the day, that laptop still left the U.S. And people might go, "Oh, is that a big deal?" Well, yeah it's a big deal. Why? If you have data loss, it implicates governments and is beyond the FBI. Now we have Indian government entities that need to be involved in any kind of a data breach or data loss situation. The other aspect of that is if there's a breach and that employee's in India, the cyber insurance policy may not cover that incident. And so the organization could be out millions of dollars. All of that can be avoided if we have not just clear policies in place, but we back up those policies with monitoring.

TAG Cyber: *Many companies have cyber insurance policies. Do most policies cover remote work?*
Podnar: I'm not a cyber insurance specialist. I actually know people who are, so I usually work with them and we create the policy and translate the organization's risk profile into a cyber insurance policy. Do most organizations automatically get covered? No. And this was true before the pandemic. Just because you had an insurance policy in place, it didn't automatically cover every individual who teleworked from home one or two days a week, or decided to go work at Starbucks because it was a more productive place for them. So most organizations need to take a look and understand the extent of their coverage.

TAG Cyber: *These days when people are working remotely, they seem to have more and more video meetings, like the one we're having right now. There are a number of potential vulnerabilities. Some of them aren't even necessarily technological.*
Podnar: Sometimes IT folks are outside of their sphere. They're thinking about how somebody might hack into the network. Will we experience ransomware? They're thinking about all the digital aspects, that we could have data loss or have an incident that we need to worry about. But a lot of times what folks are forgetting to do is think about the physical world that we're in. We are working remote, and often there are people around us. So if you go to work at Starbucks, who else can see your monitor from their screen next to you? If I'm talking to you from home right now, suppose I'm a doctor. I'm speaking in a regular voice, but next to me is my husband, who's also working at home. Who else is hearing your personal health information? We have to always be mindful that it's not just about the digital world. It's also about how it translates into our physical world, and what information can pass back and forth.

TAG Cyber: *There are lots of tentative plans for employees to return to the office. When they do, they may be bringing in personal devices they've been using remotely during the pandemic. Should their companies have another set of policies that they need to spell out very clearly at that point?*
Podnar: Absolutely. Because remember, what's happening is you're actually having not just one device but a flow devices coming back into the office environment. And often you actually don't know that device, even if it is your corporate-issue device. Do you understand if the iOS has automatically been updated? Do you understand whether all the right patches are applied from a security software perspective? Do you understand what network that device has been on, who else has been on the network? And so as these devices, whether they're corporate-issued or they're personal devices (BYOD), you really need to start thinking about how are you going to treat these things that are coming through the door that are all potentially a security threat. And then think through how you want that event to take place. Do you want people to do certain things before they come back into the office? Are you going to disable, for the time being, all USB devices until you can really get everybody patched up? Have you forgotten to disable "trusted devices" so they don't automatically connect to your network when I bring my phone back to work? There's a slew of considerations. You need the right controls. And you need to understand not just what actions you're going to take, but how you're going to respond if something does happen.

TAG Cyber: *Yeah, but you know, all I want to do is use this thumb drive [holds one up] when I get back. It's just got a couple of gigabytes. I mean, nobody would even notice it, right?*
Podnar: [Laughs] Well, it depends on your policies. For a lot of companies, they've actually disabled the ability to put in remote devices, such as a USB. And not only for devices that are coming back into the enterprise, but what might leave with that device once you stick it into the computer. Disabling those devices is really potentially important. But also keep in mind that people have a need. For you, it's your USB. How do I get this small or large file back into work? And if you don't give people a good

way of doing that, if you just say, "I'm going to disable your USB," people are going say, "Oh. OK, that's cool. I'll just put all the files on Google Drive, and I'll transfer them that way." That's not the right solution. You really do need to give people a path so they can achieve what they're going to have to achieve.

TAG Cyber: *These policies we've been talking about. Who should draft them?*
Podnar: IT has to be at the table, but so does legal. If you have somebody who specializes in privacy, get them involved as well. You're going to want somebody from the business. People go, "Business? Why am I talking to the business? They don't know anything about breaches." They don't know anything potentially about breaches, but they sure know that they can go to Google Drive if their USB won't work. So you need to understand the pain points a business is going to face, and how you're going to address those. You need to have the legal perspective to understand what you can and can't tell employees to do. You need to involve HR as well, because it's a people matter. They can also help you get the word out, and they can help you with the training aspect. So look to partner with them.

TAG Cyber: *Any last comments about the survey?*
Podnar: What's great about it is that you did create an umbrella set of questions. I think what I would do is challenge everyone in our audience today to not only look at the survey results, but ask themselves, "Can I go deeper? What are the issues in my organization that these questions might point to?" Because I suspect that just having that conversation and asking themselves the questions in your survey will get them rolling in the right direction.