Podcast: Energy + Cybersecurity – What's in the Pipeline?

June 04, 2021

You may have heard about recent cyberattacks on utility companies that resulted in large ransoms being paid and our nation's critical utility infrastructure being compromised. In this episode of More with McGlinchey, **Kristi Richard** (Baton Rouge) and **Dhruv Sharma** (Irvine) discuss what energy companies and regulated entities can do to keep consumers safe and their businesses operational and in compliance with changing governmental regulation given the ever-evolving nature of cybersecurity.

Kristi Richard: Hi, I'm **Kristi Richard** in McGlinchey's Baton Rouge office, where I practice in the Business Corporate and Insurance Regulatory sections of the firm. I'm joined today by my partner and colleague **Dhruv Sharma**, who is in McGlinchey's Irvine, California office, where he practices in the Commercial Litigation section and is a Certified Information Privacy Professional in our Cybersecurity section. Dhruv, we don't work together much, so I'm happy to get to talk to you today.

Dhruv Sharma: Thanks for having me, Kristi.

Kristi Richard: So in the recent past, we've seen long lines at gas stations, the stories and memes of people filling plastic bags and whatnot with gasoline. People being scared to drink water on certain occasions. What happened? Where did all this come from?

Dhruv Sharma: Yeah, Kristi. So if you've been following the news, there've been a couple of events in recent history, in the last few months that have really brought home the message that cybersecurity is really important to the American public. It can really affect the way they live their lives. Most recently the Colonial Pipeline, which transmits up to 45% of the fuel used on the Eastern seaboard, was the victim of a ransomware attack, which is basically, the hackers got into the system, accessed their billing records. And as a result of that, the company decided to shut down the entire pipeline. That's never happened before in its history. They shut down. It led to fuel shortages, long lines at gas stations, just like you mentioned. Essentially our entire fuel infrastructure on the Eastern seaboard was compromised. Colonial Pipeline was able to get out of it by ultimately paying up to $4 or $5 million in ransom. Even earlier in February of this year, that was a hacker attack on a water treatment plant in Florida, where a hacker breached the network and increased the amount of

sodium hydroxide in the water to dangerous levels. An operator working at the time was able to spot the attack and immediately address it. But it really raises concerns and brings home the message that our utility companies are vulnerable to cyberattacks. And it can really affect the ways we live our daily lives.

Kristi Richard: I've even seen recently a news article that says the Department of Homeland Security is getting involved and is moving to cybersecurity in the pipeline industry. What can you tell us about that?

Dhruv Sharma: Yeah, so it's really a part of a large response from the government responding to these attacks. So I know cybersecurity has been a focus for them, for the incoming administration even before these attacks happened, but it's definitely brought this into the spotlight. The Department of Homeland Security has issued directives, security directives, now requiring pipeline companies to report cyber incidents to federal authorities, and sort of moving it from the voluntary sphere to a mandatory reporting requirement. They're requiring, you know, a "cyber official" with a direct line to TSA or DHS 24/7 so that they can report an attack as soon as it happens. They're going to require companies to assess their security and compare it to mandatory cybersecurity guidelines that will be issued in the coming weeks. It's part of a broader focus by the government and the administration to really address these attacks and prevent them from happening in the future.

The Department of Homeland Security has issued directives, security directives, now requiring pipeline companies to report cyber incidents to federal authorities, and sort of moving it from the voluntary sphere to a mandatory reporting requirement.

Kristi Richard: Yeah, speaking of the administration, the Biden administration just made a proclamation, or recently made a proclamation earlier this year, on energy and whatnot. How does that play into all of this?

Dhruv Sharma: Right. So that's sort of the broader focus that I was talking about. The proclamation was issued a few days after the Colonial hack, and obviously there was a large political reaction given the impact on the public. [It was a] detailed proclamation, so it was probably in the works for some time and this event just, again, brought it into the spotlight. But it proposed a number of remedial actions that companies can take, noting up front that a lot of the utility companies in America are privately owned. So there's not that much the government can do without cooperation from the private sector. The proclamation, the executive order addressed removing barriers to the sharing of information, sort of addressing the fact that private companies may be reticent or hesitant to share the fact that they've been breached for various reasons, and moving to the mandatory reporting requirement, which again, the DHS issue that directive yesterday in lockstep with that. It requires implementation of stronger cybersecurity standards by the federal government — requiring that cloud services are secured, multifactor authentication, encryption, basic security, what they call "cybersecurity hygiene measures," making sure that the federal government and companies that contract with the federal government are adopting those.

They want to create a pilot program, sort of like the "energy star" label, you know, when you buy a refrigerator or a washing machine or an appliance, you see the energy star, and you know they're energy efficient. So they'll kind of want to create that sort of a standard where you can tell that a privately owned company meets those cybersecurity, basic security measures, especially when they're engaging in transactions with the federal government, you know, selling them software, et cetera. The administration wants to create a cybersecurity safety review board, a playbook for how to respond to cyberattacks, and ultimately sort of improve the ability to

detect malicious cyber activity on federal networks and create an event log requirement of federal departments and agencies. So a lot of different points, a lot of different measures that the government has proposed on how to these and prevent these from happening in the future. What remains to be seen is how, what specific regulations are going to come down the pipeline.

They want to create a pilot program, sort of like the "energy star" label… where you can tell that a privately owned company meets those cybersecurity, basic security measures, especially when they're engaging in transactions with the federal government.

Let me ask you Kristi, I know we're talking about the pipeline because that's the most recent hack, but there's multiple utility companies and utility sectors. Have you seen in your practice concerns from other regulated energy clients?

Kristi Richard: Yeah, absolutely. So what I have seen with my clients, I represent a couple of energy distribution service providers of electricity, both in Louisiana and a handful of other states. What we're seeing is that step-up as well. Their infrastructure, the infrastructure that's in place there, the systems that are depended upon to get electricity to the citizens of the United States, largely mimics that of the water system. And so it was a kind of an eye-opener in February. It's been an ongoing, hey, electricity, of course, is always at risk. But Florida's water hack earlier this year was certainly an eye-opener about what the energy industry and electricity industry specifically needs to do to step up their game when it comes to cybersecurity.

And just to back up a little bit, at a 3,000 or 30,000-foot level. As you said, the energy providers are largely private companies, and they are then, the distribution arm of those private companies, are governed at a state level. So it's hard to get a national impact on things that are regulated at a state level. Nevertheless, the federal government, of course, is responsible for outlining a national strategy for critical infrastructure cybersecurity. And that's going to include the nation's grid distribution system. So there are agencies, including the Federal Energy Regulatory Commission, the Department of Homeland Security as well, and the Department of Energy that are coming forward and saying, "okay, we need to make steps and have plans in order to guard against these new cybersecurity attacks."

Specifically the Federal Energy Regulatory Commission (FERC) took a major step earlier this year or in 2020, rather, end of 2020, incentivizing these private companies to bulk up their cybersecurity investments for those public utilities. As a standard, they have to meet Critical Infrastructure Protection, reliability standards, or CIP standards. And that's the bare minimum that they have to do, mainly dealing with the reliability of their services, making sure that they reliably get energy and electricity to their customers. What FERC is doing to incentivize more cybersecurity investment is taking those standards, some of these standards there are not applicable to every industry, or not applicable to every facility, rather. And so if there are voluntary parts of that, that they don't mandatorily have to comply with, if you're doing it voluntarily, that can get you some incentives. Or if you meet higher standards and guidelines from the National Institute of Standards and Technology (NIST), that can also get you these incentives.

What FERC is doing to incentivize more cybersecurity investment is taking those standards, and if there are voluntary parts that they don't mandatorily have to comply with, if you're doing it voluntarily, that can get you some incentives.

The incentives are one of two things that you can choose from, being a rate of return adder of 200 basis points, or deferred cost recovery for certain cybersecurity-related expenses, including things like if you're paying a third-party vendor for hardware or software, or computing networking services to get those up to speed, any kind of expenses for trainings to implement those new cybersecurity enhancements, or other expenses such as risk assessment. So trying to have a third party hack into your system so that you know, that it can't be done. So mimicking you, Dhruv, just saying they're, everyone, the federal government is taking notice. They are making sure that these companies comply, number one, and even incentivizing them to enhance those cybersecurity methods.

At the state level, I haven't seen too much so far about cybersecurity because they're letting the federal government handle it, especially the Department of Homeland Security, Department of Energy, and whatnot. But what really the state-level public utility commissions, who are the ones that regulate these public utilities and private corporations, are focused on is data privacy of consumer information, which is similar and related, but not exactly the same cybersecurity stuff. So that's what they're concentrating on, but it's going hand in hand. If that information can't be hacked, well, then you have another step, of course, the basic step toward protection against cybersecurity hacks that could lead to the complete energy grid going down.

Dhruv Sharma: Yeah. And there's a number of factors that sort of put it on the federal government's plate rather than state governments', right? So these are oftentimes these are out-of-state actors, foreign actors, sometimes state-sponsored actors based abroad, you know, hacking our infrastructure systems, really compromising our security, essentially. Utility companies cross across number of states, so a company shutting down in one state, in Louisiana may affect the fuel shortages on the Eastern seaboard or on the west coast. So the footprint of these cyberattacks is massive and it truly is a security problem from a domestic standpoint.

So we've talked about Kristi, how the government is responding, what should your clients and my clients, what should our clients be doing in response to this? What are the operational sort of advice that you would give to them?

Kristi Richard: One of the funnier contracts that I've had the opportunity to look at recently was a contract between one of our clients who's in the energy space and social media aggregator. It pulls all the times that this client is mentioned on social media, anytime customers comment on any of their posts or on their pages or whatnot on social media, and anytime that they've commented back, and the like. And we went round and round and round with their attorneys, trying to make them understand [that] not only is this energy provider Uber-regulated by the states, and by the federal government or whatnot. They have heightened security, cybersecurity and data privacy protections, and that they needed to also comply with these. Of course, the social media aggregator says, "well, we're just pulling the information in. We don't have access to personal information of the customers or of this client that they were trying to provide." [Let's say] there's an outage in your area. They may go on social media and say (blips name) "hey, my power is out at 123 Main Street, Baton Rouge, Louisiana." And that's giving away personal information there. Even though the consumer's done it, you don't want someone to be able to come in, easily identify that information, and then it some way go back to our client and have them responsible for that information being there.

So you need to understand not only what cyber insurance is, but what particularly that you need and what particularly is going to be covered in the instance that you're attacked.

Another thing that our clients can do, and in general utility companies can do, is look into cyber insurance. This has been on the uptick lately, and I'm glad it has. It provides some protections, but you also need to know what you're getting. You need to have a good relationship with your broker so they can explain to you. What's exactly covered? Like we mentioned in the Colonial Pipeline instance, they had to pay between four and $5 million to get their information back. Is your cyber insurance going to cover that? Is it going to cover actual Bitcoin? Do they have a Bitcoin bank kind of policy, and access to that bank that they can pay it for you? Is it going to pay for the restitution that you'll have to pay for your customers or in a data breach, such that if you're paying for their credit monitoring service or something like that, in addition to the lawsuits or class actions that you might inevitably get because of this data breach. So making very sure that you understand, not only am I protected, but what I'm protected against. Is it different from if it's an internal attack versus an external attack, meaning did one of your employees go in there and get something that they shouldn't have and disseminated it? Did it come from outside your company? Did it come from outside of the United States? Like, you know, Russian hackers, like we saw in Colonial, or inside the domestic United States? All those things are going to be spelled out there. So you need to understand not only what cyber insurance is, but what particularly that you need and what particularly is going to be covered in the instance that you're attacked.

Dhruv Sharma: Great points, Kristi. And one of the great benefits of cyber insurance, and one of the incidental benefits, is that each insurance provider is going to have its own standards and requirements for cybersecurity within the company before they agree to insure it. I mean, you know, your premiums are going to depend on it, and before they agree to commit millions of dollars, potentially, to cover you in the event of an incident, they'll want to know that you're taking the necessary step to protect yourself from a cybersecurity hack. So it provides you the sort of trial run test, almost, to see if your protocol is up to speed. And, you know, if you're well protected just from an industry standard on cybersecurity.

Kristi Richard: Absolutely. What the underwriter is going to look for in determining, number one, if it's going to insure you, and number two, what your premium rates will be, is doing that deep dive into your system. So although you're paying a premium, the actual insurance premium for it, it is almost a free attack on your system to see where the vulnerabilities are, and getting in there, finding your weak spots. So it's definitely that added protection or added kind of knowledge that, you know, not only am I protected on the back end because I have insurance that will help me do this, but a little bit, a little bit more protection or a little bit more knowledge that, okay, we've done what we are supposed to do, or we've done everything that we could to try to prevent it in the first place as well.

Well, Dhruv, I've enjoyed talking to you today. We don't always get to work together too much, being in different offices and in different sections. But I think this is a great place where we kind of showed that there are so many cross relationships between business, between cybersecurity, and commercial litigation as well. And I hope that our listeners have learned some good points. I certainly have listening to you, and I hope we can talk again soon.

Dhruv Sharma: Thanks for having me, Kristi. Likewise.

download transcript

get more episodes

Subscribe wherever you listen to podcasts:

Related people

Kristi W. Richard