Rachel Johnson, Cherryland Electric Cooperative (00:15):

Welcome back to another episode of co-op energy talk. I'm your host, Rachel Johnson, the member relations may manager here at cherry land electric cooperative. And I recently got an email from a member and in it he said, are you ready for the Russians? And it was kind of like a really jarring start, but he went on to inquire about tray land, cybersecurity readiness, and it was clear that was something he was concerned about. And it's a fair concern. And it's certainly one that is top of mind for a lot of people today. Increasingly we use digital technology to control, monitor, maintain the transmission and distribution of power. These advancements have made the power grid more reliable and more robust. Certainly our members have seen that and are benefiting from it. It's a very good thing, but as we increase the interconnections among these previously isolated parts of the grid, and we implement digital technologies that automate grid functionality, it exposes the power hour grid to many of the same cyber security vulnerabilities that haunt other businesses.

Rachel Johnson, Cherryland Electric Cooperative (01:06):

However, in our business, a cyber attack could result in disruptions and wide scale power outages with extensive social and economic consequences. So it is, uh, it is a sincere concern and it is one with significant consequences. I recently sat down and recorded a podcast with cherry lands, general manager, Tony Anderson, and Dr. Emma Stewart, Dr. Stewart is the chief scientist at the national rural electric cooperative association, or N R E C a. She leads the business and technology strategies team there, which focuses on grid, reliability, transmission, and distribution, and cyber security prior to coming to N R E C a Dr. Stewart worked on defense infrastructure at Lawrence Livermore national laboratory, and also manage the grid integration group at Lawrence Berkeley national laboratory. She earned her PhD in electrical engineering and a master of engineering from university of Strat Clyde and Glasgow Scotland. So basically what I'm trying to make sure you are aware of is she knows her stuff.

Rachel Johnson, Cherryland Electric Cooperative (01:58):

And when it comes to cybersecurity, she is someone who is very, um, knowledgeable, incredible, and talking about the risks to our electric grit. So that's, that's kind of what we discuss with her, what we, what risk we should be concerned about and also how we can as utilities, but also as a society work to mitigate those risks. So here is our conversation with Dr. Stewart and Tony Anderson. Well, Emma, thank you very much for taking the time to join us today and talk about this issue that we know is really top of mind for a lot of people right now. We appreciate your time.

Dr. Emma Stewart, NRECA (02:25):

Nice to meet you all.

Rachel Johnson, Cherryland Electric Cooperative (02:26):

Yeah, well, and we're our, I, I know our listeners are excited to get to know you, and I think we'll just dive right in, uh, with kind of a really broad question, but can you just talk in general about what the cybersecurity risks are to the nation's electric grid?

Dr. Emma Stewart, NRECA (02:38):

That's a, a pretty big question nowadays, given everything that's been going on geopolitically as well. I think everybody is aware, um, if they haven't been made aware, they should probably start watching the news of some kind that we've got a fairly large issue going on in, in the other side of the world right now there's been increased, uh, IP attacks, essentially people trying to probe different people's systems

recently, um, coming all from addresses across the world. It's essentially people are looking for holes at the moment. They want to find a path into people's systems. And, and they're looking for that just now, but sort of brought more broadly. Um, the electric grid is one of those really interesting places that it, as in the business systems and opera regional networks, both are running, um, at the same time or both are generally essential to keeping the system online.

Dr. Emma Stewart, NRECA (03:24):

So even when we are hearing about things like ransomware or other kinds of attacks on the system, that still has an impact on energy delivery, um, it still affects our ability to do business so broadly groups. Um, our it and OC convergence is one of the, the bigger risks at the moment on the electric grid. The more we start to look at things like integrated distributed resources and other PC like that, the more, the more connectivity we have with every device, um, such as people managing to put tweeting printers onto their network. Um, you know, there's, there's just a lot of increased risk at the moment coming and from all of that, but there's also a lot of increased, uh, access to new things and communications and things that we really need to move the world forward. So we definitely need to sort of balance that risk as well with the benefits of increased communications overall.

Rachel Johnson, Cherryland Electric Cooperative (04:12):

Sure. Yeah, it's it, it, well, the risks are there, they're there because of a good thing that has made the grid more reliable and in many ways more resilient and we can do more things with, but also we've got rid of some of these isolations by connecting things to one another. And that means just kind of awareness of, of how to best manage some of those risks you described.

Tony Anderson, Cherryland Electric Cooperative (04:28):

If you had to PR prioritize those risks, how would you do that? What's one, two and three.

Dr. Emma Stewart, NRECA (04:34):

The biggest risk at the moment is really on the O if I'm talking about the biggest impact of something happen, it really is our operational networks and our industrial control systems. As we start to, to modernize the system, those are definitely becoming more of a, both a risk and benefit. We want to control more things. We want it to be more efficient, but not, that's probably number one is the OT side of the house. I think that's one of my bigger concerns at the moment, moving down sort of ransomware and things like that do have a massive impact from the economic standpoint, people have been getting very large ransoms and that has ongoing impact. That's probably my second biggest concern is what happens during ransomware and, and the cost of that. And the last risk is to everyone is generally just simple human issue with being able to click on emails, understand what you're connecting. I'd say that's actually probably could be number one, as well as humans essentially are one of the biggest risks to the grid because we, we interact with it all the time. And we don't always know we're interacting with it through that computer where you accidentally clicked on that link saying, here's your gift card, or please join the space force. So,

Rachel Johnson, Cherryland Electric Cooperative (05:39):

I mean, I'm always sure I'm gonna win just to be clear.

Dr. Emma Stewart, NRECA (05:42):

Yeah, I need to it's okay. But you know, I, I get it. Some of those emails are became fairly sophisticated recently, so, you know, it's been

Rachel Johnson, Cherryland Electric Cooperative (05:49):

Difficult. It's crazy. And I'm gonna actually turn this over to that same question to you, Tony. But before I do, I just wanna make sure for our listeners that maybe aren't in the biz, you mentioned ICS, which refers to industrial control systems. And those are basically just the systems we use to manage electrical processes and physical functions in the grid like opening and closing circuit breakers. And we can do that now from our office because we have connectivity out to those things. So when we talk about ICS, that's what we're talking about. The things we use to actually operate the system, oftentimes from inside the office, but now Tony, you, you you've managed cherry land for a really long time, really long time, a really, really long time. Uh, so I just want you to kind of also answer that question. Like if you had to prioritize the risks as it pertains to cyber security, what are the biggest concerns to you?

Tony Anderson, Cherryland Electric Cooperative (06:30):

It's absolutely the distribution automation, which Emma, uh, mentioned 19 years ago when I came to Len, nothing was hooked up to the grid. You know, we, we hardly used the grid for automation, meters. Weren't hooked up substations, weren't hooked up. And now every month we're, we've got 16 substations on fiber, 16 substations with automated controls, and we're moving down line with automation and we're hooking that up to fiber. So we have more and more opportunities as every month goes by to be attacked and to be vulnerable. Um, when I started in the business in 1983, nothing was connected there. The only vulnerability we had was a car running into a pole or a substation and squirrels. And it's squirrels. Now we're worried about people from across the ocean. Tapp,

Dr. Emma Stewart, NRECA (07:20):

Spoils are still number one, right? So

Tony Anderson, Cherryland Electric Cooperative (07:22):

They will always be number one, they will always be number one.

Rachel Johnson, Cherryland Electric Cooperative (07:26):

So, I mean, I think you've, you've both got us scared. So congratulations. You've done that part of the podcast. My, my, my next question is, okay, what measures are in place right now to mitigate those risks that people should be aware of so that they can at night. And I don't know, Emma, if you wanna maybe take that one first,

Dr. Emma Stewart, NRECA (07:42):

One of the, the biggest things we have is, is knowing what's on your system. We have tools now available where you can actively see what is connected to your system. What's talking to what, as in, if something is talking to its neighbor, you probably want to know about it. So we do have these tools available. And one of the biggest things I think is there, is being able to know that self and be able to do a self assessment of where your system is at and know what your biggest problem is. You can do a, essentially a roadmap of where you're going in cyber and, and know what you need to do for the next few years. I think that's one of the, the sort of biggest measures that are in place that being said there has recently been a fairly large are just sort of whole of government approach to trying to improve this situation, obviously, in response to the current situation, geopolitically, um, DHS DOE um, all working

together to essentially try and work out the best scenario to improve or bring along the security of the electric grid.

Dr. Emma Stewart, NRECA (08:37):

And it's not just, co-ops, it's, it's everyone trying to, to move ahead and to get to the next step of that, that security level. So there's all sorts of ways just now to be able to take action in those findings. Um, there's people are on top of vulnerabilities, more so than they ever have been. Um, unfortunately that also means we get emails from people like IAC, which is our electric sector information sharing advisory center. So they will send you emails daily, um, sometimes early to tell you what the next thing is. But all of that is from this like whole of government approach just now to try and really bring all of the us L electric systems to that point where we're comfortable and secure. Um, but it's a constantly moving target, so things need to evolve, but EISAC is one of those big solutions, as well as being able to send out information to everybody about vulnerability or an attack or an event, even both across physical and cyber systems, or even just the risk of that happening is, is a very valuable resource as well.

Tony Anderson, Cherryland Electric Cooperative (09:38):

What would be a worst case scenario or two that a utility should be prepared for?

Dr. Emma Stewart, NRECA (09:44):

Ah, that's my, I like talking about worst case scenarios. I, I did a lot of, uh, in my previous life, I did quite a bit of things that we're talking about. Like worst case scenario planning. My, my husband hates, um, actually I contingent planner. I have 10 different plans in place for everything. Um, but the thing we want people to plan for just now is the real potential that by no fault of their own, um, with all protections in place that the light still could go off and that could be caused by a cyber attack. And that recovery could take a bit longer than your planning. Um, there's new processes in place for recovering from that, but that is, that's the thing we are planning for at the moment of what, what do we do from the N R ECA side, if something like that is actually happening. I mean, that is really the worst case scenario is the, the lights going off

Tony Anderson, Cherryland Electric Cooperative (10:30):

And say the, that does happen. And the lights do go off. What's the worst case scenario for how many days that we're it take to get them back up?

Dr. Emma Stewart, NRECA (10:38):

So I, I worked on, uh, DARPA had a program for this that was called Redix that we did run through these scenarios in seven different exercises, um, where we'd run through. I think at that time it was three days for people to actually get together and actually work out that this is a cyber attack and we need to do something differently. Um, risk sponsor services coming from different areas like activating national guard is one of the big responses. At that point, they have a cyber response team that will come and help as long as they're activated. But I will say like, we plan for everything from five to 14 days when we're talking about this kind of recovery, mostly if it's around the first times, this is happening, then people are gonna earning how to, to bring it back as well. So it's yeah, not to be dimming Glen though. There are tools in place to help. Yeah.

Tony Anderson, Cherryland Electric Cooperative (11:24):

Yeah. I, I wasn't scared until you said 14 days.

Dr. Emma Stewart, NRECA (11:28):

No worries.

Rachel Johnson, Cherryland Electric Cooperative (11:30):

But I think Miu makes such an important point, which is in that scenario, it's so important that we have a coordinated response that include both local utilities and also whether it's national guards, state level response, and federal level response. So this work that you just described that you're doing, hopefully at least prepares us to maybe figure out what's going on two days in instead of three days in because there is good coordination. And, and maybe some of the, the global events you talked about earlier on are bringing this more to light and hopefully, um, reiterating the need for resources there. But assuming we don't end up in the catastrophic worst case lights off event for 14 days, what are kind of the more, um, likely and real everyday types of cyber risks that utilities need to manage?

Dr. Emma Stewart, NRECA (12:17):

The most common thing I, uh, yell at people about at the moment is Phish emails. It's still the most common way people are getting into people's systems. Um, I think Tony has heard me have these conversations at various different events where I, I play again to try see five times he got to hear like who's counting in every regional meeting. He got to hear my little joke of stealing people's passwords with simple questions on Facebook. Yeah. Um, those kinds of risks are really the, the highest problem at the moment. They're the thing that's more likely to cause somebody to get into your system. It's human factors clicking on emails. Again, I make that joke about joining space force. That's one that our people used on us, like join the space force, go to the Martian academy. And I didn't click on it bit. It looked quite realistic. It was and interesting as a future career path, but you know, it's

Rachel Johnson, Cherryland Electric Cooperative (13:09):

Well, and it, it's just, it's hard because as humans, we wanna connect with other people and that makes a vulnerability, a human vulnerability, right? Someone emails me something I wanna respond to it. Someone puts a whatever, remind us where you got married post on Facebook. And then I wanna tell them that in my birthday and the next thing you know, they have access to my bank account. But yeah, no, the human side is definitely interesting. And we do, we do quite a bit on that at cherry land, but Tony, can you talk about what we do kind a to day here for some of these issues?

Tony Anderson, Cherryland Electric Cooperative (13:36):

Sure. Uh, Steve Weaver is our it manager and he, he works on this every day. He also participates in N ECA work groups on, uh, cybersecurity events and risks and what to know. So Steve is a big thing. We, we have a lot of our eggs in the Steve Weaver basket and, and he does a good job monitoring our systems 24 7. A lot of that's automated, as far as the fishing stuff. For average employees like me, we, we use a company called no before and they give us simple little tests and they test emails and teach us when in doubt delete. So that's a, that's an ongoing thing. You never know when you're gonna get one of those. And that's a good thing so far, I haven't clicked on so wrong. So knocking on wood, doing my part. Uh, we do a monthly board report to the board on cybersecurity and what Steve has done over the last month and, uh, what he's found and what he's worried about and what's coming up.

Tony Anderson, Cherryland Electric Cooperative (14:29):

And, uh, that's been very helpful to keep the board up to speed on cybersecurity. So, uh, when it comes time to budget, they're more informed. And, and that, that helped us out. Uh, recently, like last year

when we did our budget, we added a new it employee that we're currently in the process of hiring. So we don't have all our eggs in the Steve basket, or we can give him more time to donate to cybersecurity and less time to do the, the, the small stuff. So a lot of moving pieces going on, but we, we have a lot in play.

Rachel Johnson, Cherryland Electric Cooperative (14:59):

Yeah. And I think a, another piece of that, Tony is that co-ops and the people we serve, cuz we, we serve them at cost need to understand that the, the cost of making sure we are prepared for a cyber security event are going up, but it's the right thing to do. And we have to invest in that. And I don't know, I don't know someone here said this first and who knows Emma, maybe they heard it from you, but kind of whatever you're paying today for cybersecurity is the least amount you'll ever pay. Cuz it's only going to become more and more important, but something we need to invest in and kudo store board for doing that. And certainly to our staff,

Tony Anderson, Cherryland Electric Cooperative (15:30):

I heard Jim Mathis and the CEO of our national trade association, N R ACA uh, say this just this week that it staff is the most competitive, uh, sector of our business right now because everybody, they could always work from home and now they can work from home more easily and it's a highly competitive for good it people. And that's where we're, we're struggling a little bit.

Rachel Johnson, Cherryland Electric Cooperative (15:55):

Yep.

Dr. Emma Stewart, NRECA (15:55):

That is a, that is a big point. The, the, the workforce challenge at the moment, I think department of commerce reported there's I think I believe 500,000 open positions in the it and OT space for security and, and in general for it, it's just, it's astounding how many jobs there is needed and how little people there are just now. So everyone's definitely wearing multiple hats.

Rachel Johnson, Cherryland Electric Cooperative (16:18):

Yep. Yep. And then, I mean, and for all of our employees listening to this, that's why it's even more important that you don't click on things. So just we have to, we have to help them out be the frontline. So Emma, in general, what, what changes do you think that we either as a nation or just as a utility should be considering in order to best defend ourselves against cybersecurity risks,

Dr. Emma Stewart, NRECA (16:38):

One of the top changes or top I'd say improvements, um, would be getting used to sharing information with your federal partners or with your information sharing partners there's been in general, people are, you don't want to admit, you're the one that it wrong. Like you don't want to admit that you had the, the, the event on your system, but often if that's done in a speedy and timely way, there can be information shared with people across the nation that could prevent the same thing from happening to them. And so that's kind of the, one of the, the bigger ones just now is people getting more comfortable with sharing it with people like EISAC, for example, um, potentially with this new information sharing law, there might be requirements to do that. I know we're working with DHS on helping shape what that actually looks like. But again, that information reporting, volunteering that up even anonymously can, can really help.

Dr. Emma Stewart, NRECA (17:30):

That's one of the bigger changes I think we should consider. I keep saying it, please share your information with the ISAC or even just tell me in various cases and I will help you with that. But sharing with the ISAC is one of the, the bigger things for the electric sector in particular, there's other ISACs for other areas as well. Um, I will see, I think the increased monitoring is also really helpful, like knowing you're even just being probed or somebody is looking at you, I is very helpful. There's open source tools for doing that as well. Things like Showan, you can, you can find out if your information is folding around out there. Um, those kinds of things are, are useful as even just to serve basic level of, of knowing where your parameters at is helpful, which

Rachel Johnson, Cherryland Electric Cooperative (18:11):

I would also, I would assume help you kind of get some trend lines over time, so you could recognize, whoa, there's something really has shifted. Like we we're experiencing a significantly higher amount of attacks or whatever, but your point about information sharing is a good one. And one, I take to heart as a, as a public relations person, because I think our, our natural tendency is to say, whoa, a crisis is a happened, like circle the wagons figure, figure it out. And then, and then when you're ready, kind of communicate it. But, but this is, uh, clearly something where that coordination we talked about earlier is, is really important.

Tony Anderson, Cherryland Electric Cooperative (18:39):

I kind of have a follow up to that last question. Can you talk about the pace at which technology is changing and how that might impact the way we think about and prepare for cyber attacks?

Dr. Emma Stewart, NRECA (18:48):

I mean, I I've worked in integrated technologies now for 15 years. I think we started on some of the like smart and vector communications probably 15 years ago that that was starting. But I would say the pace of this is increasing drastically right now. Um, there is a definitely an exponential increase in the number of communication points we have on the system. I believe there is laws that talk about that. I actually like MES law, different things. Talk about the speed at which things are starting to talk to each other just now, um, I'd say that the technology for monitoring definitely on the it side there's, it's moving pretty fast on the OT side. They they're catching up at the moment. I think people weren't necessarily sure where that was and a couple big companies really start to you to push it forward. And, and now I think we're, we're gathering pace on the operational network security as well. Technology though, people accidentally connecting things to their network is still a challenge. And I think that's, that's one of the bigger ones. Um, that technology, I still don't know why my fridge can tweet. I have no idea. I know that like people seem to like at being a feature and it, it is one of the bigger problems. Like why do we have unnecessary communications connected to networks? It's unclear. Um, it's just in environments where it's critical. That's a good thing to be careful about. Don't connect your printer to the operational network.

Rachel Johnson, Cherryland Electric Cooperative (20:05):

So to the electric grid. Yeah, yeah, yeah. And it, and it's interesting because in, in this goes to the idea of like the it in the bad, right? The internet of things has created a lot of really amazing opportunities in our lives. And at the same time, the more we lose those kind of that separation between these key operational pieces. And, and to your point, like, yeah. So if I'm suddenly able to, you know, whatever load control your refrigerator, for example, which we wouldn't do, but your water heater, what ever

then now, anything that comes through your water heater is now communicating with the grid and that, that that's also a vulnerability. So thank you for that point. Um, so as we kind of wrap up our, our podcast, I just wanna reiterate, we know, we know there's a lot of fear and anxiety right now about security of the grid, and there's all, you know, a lot of media around it clearly partially in response to some global things going on. Some of it's real, some of it's probably over inflated. Some of it may be understated. I don't know, but I, I would just love to hear if you have any final takeaways for our podcast listeners, as they think about how to have a reasonable perspective, what are, what are the vulnerabilities and, and kind of, what does the future look like for the, the security of the grid?

Dr. Emma Stewart, NRECA (21:12):

Well, we're definitely in a, a case of fear and anxiety on some of this just now. Like I watch the news myself and I have the same, some of the things they say, I have a definite eye roll on, cuz I'm like, oh, okay, well maybe I will say like, there's a lot we can do. And I think the us still has never had an actual operational outage caused by a cyber tech it's not happened. So that being said, it doesn't mean it won't. And I think the best thing people can do is plan for it just now. Like we want people to have really solid, uh, cyber instant response plans. We want people to exercise those plans essentially just assume at some point that that would happen. And your response is actually more important than what happened in the first place. In that case, your response is everything. So making sure those instant response plans are tested is, is one way to remove that anxiety. Cuz at least if you have something in front of you, that's giving you some of that guidance of who to call when it can remove some of the panic. When, when it does it a ransomware event or an operational event, having that plan, there is one of the greatest things people can have at the moment.

Rachel Johnson, Cherryland Electric Cooperative (22:15):

That's, that's such a good point and you know, the, the wrong time to make a plan is when you need it. So, um, that's a, that's a well made point. Tony, do, do you have any final thoughts for our listeners on, on this topic area?

Tony Anderson, Cherryland Electric Cooperative (22:26):

I'd just like to assure them that we do take this and we work on it every day, literally every hour of every day, we're we're monitoring our risks. And I, I agree with Emma. What helps me sleep at night is the fact that it hasn't happened yet. You know, we we've had years of this and it is increasing, but it hasn't happened yet. So every day it doesn't happen. I count that as a win and winds are good. So we're gonna take mini of, as we can get and try to prevent it from happening in the future. And the other thing I'd like to the listeners to remember is cherry land is connected to the grid more and more every day, but there's a lot of rural America that is not yet connected to the grid. There's a lot of small co-ops out west and in different places, rural areas of the country that are not automated yet.

Tony Anderson, Cherryland Electric Cooperative (23:11):

So the, the risk for them is small. Cuz until you hook up to the grid, you don't have the risk. And so that, that will continue to grow as the years go by. So we're gonna learn a lot now that will help those co-ops out later. And the other thing I like to tell people a little bit tongue and cheek, but when we're outta power sore, the bad guys and do the bad guys really wanna be outta power. They're not lugging a generator from town to town or apartment department. They want power. So it's more likely a ransomware attack than, than the power going out is what I try to tell myself when I get a little anxious.

Rachel Johnson, Cherryland Electric Cooperative (23:45):

Well, I, and I, I, I just wanna reiterate how grateful I am to both of you for taking the time to talk about this. And um, I know clearly Emma, you have a, a ton of experience and expertise in this space and it is something that we take really seriously here at cherry land. And it was really important to us to do this podcast right now because we want to make sure we are communicating with our members and we are transparent with them of about the challenges we're managing, but also that, um, hopefully this can give our listeners out there a little bit of confidence that we remain committed to keeping the lights on and doing whatever is necessary to make sure that is true, including working with our national partners on cybersecurity issues. So thank you. Thank you both for joining me today to talk about this issue. Thank you.

Dr. Emma Stewart, NRECA (24:22):

It was nice to

Rachel Johnson, Cherryland Electric Cooperative (24:22):

Chat with you. It was nice to chat with you as well and for our listeners out there. Thanks for listening. Join us next time for co-op energy talk.