Courtney Doyle (00:18):

Welcome back to another episode of Co-OP Energy Talk. I'm Courtney Doyle, communications and member Relations manager at Cherry Land Electric Cooperative. Today, we are diving into cybersecurity. It is a complex, fascinating, sometimes a little frightening topic that is top of our minds here at the cooperative. And today we have the pleasure of talking with cybersecurity expert Patrick Kelly. Patrick founded two cybersecurity organizations, larist Security and Critical Path Security. He is an ongoing cybersecurity expert for NBC News. He's spoken on panels alongside the F-B-I-C-I-A and NSA. And recently he's been making the rounds talking to electric cooperatives about this increasingly important topic. So listen in as we dive into talk cybersecurity and what it means for your utility and your co-op. Patrick, thanks so much for taking a little time to join us on the podcast today to talk cybersecurity.

Patrick Kelley (01:15):

It's great to be here. Thanks for inviting me.

Courtney Doyle (01:17):

Yeah, we appreciate it. So, cybersecurity is such a broad, kind of intimidating topic because that goes in so many directions, and I feel like it's always changing. So can you first just start by telling us a little bit about yourself, what you do, and the organizations that you created?

Patrick Kelley (01:38):

Sure. Um, I'm a 25 year, almost 30 year veteran, um, in IT and cybersecurity. Um, you know, at this time, you know, I've used that experience to, you know, build two companies. One is critical path security. Um, we're using that as a professional service company to help EMCs and co-ops that are struggling with how to build cybersecurity programs, um, in the organization and in this day and age, and with the evolving threats that they have. And then with liga security, um, as a platform that we created, which is really a consolidation play, um, most of the EMCs and co-ops were really being tasked to, to buy a, a bunch of different point solutions and, and all together, they couldn't really afford them and they couldn't afford the training. So the goal with lyricists was to bring a lot of that functionality into one single affordable deployable solution to help, you know, organizations improve their security posture and, and, and having a chance to defend themselves.

Courtney Doyle (02:38):

It's crazy how many sectors, I guess, right? It touches Cybersecurity touches us at home, it touches us at work, <laugh> at and as a utility. I, I've had the chance to sit in and work a little bit as Cherry Land was building our cybersecurity incident response plan or our serp. Um, and it really opened my eyes, you know, I'm there from kind of a, a crisis response, crisis communication standpoint. But then, you know, we start diving into how all these things intertwine. Can you talk us through a little bit about cybersecurity concerns, specifically in the utility space and how, you know, not not just your normal office cybersecurity stuff, but how it intertwines with the grid and everything like that really blew my mind.

Patrick Kelley (03:24):

Yeah, so EMCs and co-ops and utilities, it's a very interesting place because it's very different than what we see in other, other parts of, of other industries, in other parts of the world. Um, you know, if, if you're looking at a Coca-Cola or a FedEx or a UPS or a Delta, you know, they're updating their infrastructure every five or six years, um, some things even quicker. And that's just not how it works In EMC and co-ops, um, you know, we're building substations and we're building, um, transformers and things that we hope to last for 20 or 25 years. And most of these things were never built with the intention of being put into a hostile environments. So they're not hard in that way. The other is the challenges that are just to EMCs and co-op from cybersecurity point of view as they stand, which is it, it's really hard to pay employees competitively in EMCs and co-ops when you're comparing it against that private industry such as, you know, again, the Home Depots, the Deltas, uh, those large orgs where increasing, you know, the amount of money that you can pay somebody or having more flexibility and, and the CapEx and the opex just isn't there.

Patrick Kelley (04:33):

The other is that most EMCs and co-ops, you know, they have a person, and especially in the United States that does all of the cybersecurity, they handle all of the, it, they handle everything from compliance, um, regulatory across the board, and it's, it's one person that has to be, you know, incredibly well versed and successful, you know, in that one theme. So it, it's, it's really tough. And the lack of the, the last one that I would bring up is with the brand new, um, federal regulations, and there's another one that just crossed my desk today. It's requiring these mandatory reporting times and 24 hours, um, simply is, is not enough even for a well-funded organization to understand what the impact is of a ransomware event. These things take, honestly, weeks, if not months, for an organization to get their head around. So, you know, we have a, a lack of funding, um, which I'm not blaming on, AMCs and co-ops say how how AMCs and co-ops are paid is, is quite different than what you see in the private sector.

Patrick Kelley (05:40):

Um, we have a lack of cybersecurity staff and when we can get them, you know, the pay just isn't what it is in other places. I think since it's conversational, there's, there's something that I, I think it's really important that I missed. EMCs and co-ops are your gateways into the larger organizations. So I paint that picture real quick. Your global threat actors and your nation state actors, uh, be it Russia, China, North Korea, they're not gonna go straight at, you know, Georgia Power or, um, duke or Alabama Power, or these larger ones because they know that they have, you know, a very large budget and they're very well placed and they can defend themselves in, in, in ways that are quite different than an EMC and co-op. But there are typically trust relationships between the larger, the g and Ts and EMCs and co-ops. Cherryland is as well as many other, or the smaller EMCs and, and mid-size, EMCs and co-ops are targeted by nation state actors in a way to get into the g and t and then use that g and t to get into the other EMCs.

Courtney Doyle (06:48):

Yeah, so like a, a gateway or kind of like practicing, right. Like <laugh>.

Patrick Kelley (06:52):

Yeah, it's a very, it's a very interesting and a very intelligent way to go about it. Um, and it's very tough to stop with the, with the budgets that most EMCs and co-ops have.

Courtney Doyle (07:04):

Yeah. So it's, it sounds like the first step for a lot of co-ops may be starting to invest in this space and having it more top of mind. I know at Cherryland, we just recently did a little bit of a reorg where our IT and our ot, our operational technologies teams, you know, now they work under one umbrella, and that gave us some space to take one of our traditional IT staff members and, and have a cybersecurity administrator, somebody who can dedicate all their time to watching this legislation or these new, um, regulations or just monitoring, right, right. Monitoring how often somebody's trying to breach our stuff or how often we're getting those attacks and things like that. And then where, and getting to really dive into the, the data behind it so that we can invest in the places that we need to invest. Right. So what I'm hearing you say is that investing is kind of that first step. Um, as far as time and resources. What do you think, you know, if, if co-ops were able to spread their tools out a little more and invest in that, then what would a next step be for a co-op from there to work towards hardening, I guess, uh, the grid or hardening our cybersecurity as an organization?

Patrick Kelley (08:25):

That's a really great question, and I'm probably going to provide a, a, a very, a typical answer <laugh>, um, from the point of a, a cybersecurity vendor at least, um, you have to choose where you, where you spend your dollars wisely. So the first thing that I want to do, if I were going to be that one cybersecurity company and a property EMC, is let's take an inventory of what we have. And I've come to find that most organizations, co-ops and EMCs will have some overlap in the tools that they already have, and they just don't know, uh, 'cause they haven't, they really haven't had enough time to properly train themselves on it. So the first thing I like to do is, is say, okay, what do we, what do we already have and how can we use it? Do we need to go buy something else?

Patrick Kelley (09:15):

You know, or, you know, do we have, we just not had enough time to develop a proficiency in the things that we have. At the end of that, most EMCs are gonna, in co-ops, are gonna find that there are gaps. So we want to intelligently apply those funds into those gaps, and maybe we apply that 80 20, you know, percent rule here. Here's where I'm gonna challenge sort of the, the, the, the traditional view of cybersecurity. I, I don't actually believe that most EMCs and co-ops need to go out and buy the best of breed tools for everything. At the end of the day, if you're gonna best of breed at all, you know, you're gonna have on average about 17 to 18 different platforms that you have deployed. That means that each person that's working in that part of the organization has to become an expert on 17 or 18 different platforms on top of everything else that they're doing that's not feasible.

Patrick Kelley (10:11):

Um, so you are gonna find that some of the things that you bought aren't deployed properly and they're, they're configured wrong. Um, quite often we find that organizations will go buy something, they won't properly configure it, and it will actually increase their attack surface as opposed to making things better. So I'm a very, I'm, I'm a very big fan and I have been for a long time of, of getting all you can out of what you have. And when you're looking for other tools or platforms and things like that, you buy things that can do a whole lot so that that one person that just got the job has a, has a fighting chance of, of learning how to do it. If, if you, if you think about a plumber, let's demystify cybersecurity for a minute. So I, I don't feel as cybersecurity is, is entirely indifferent than being a plumber.

Patrick Kelley (11:04):

We have to get things from things to, to, from one place to another place. We need to protect it as much as we can. If it's water, you know, we wanna have it in pipes and we wanna make sure those pipes are strong and we wanna make sure that those pipes aren't going to break. We can't see everything. You know, some pipes are in drywall. Drywall, and, and you've gotta, you, you've gotta make some decisions and make some abstracts and things. You know, if I go to a plumber and I give him a hundred different brand new shiny tools, but I don't teach him how to use a rich, what's the chances that he's going to be able to fix a problem? Or he is going to be able to move water through my house without there being a water leak or a break or something devastating.

Courtney Doyle (11:48):

Not great. <laugh>

Patrick Kelley (11:49):

Not great, right? Um, the other thing is, um, and what's incredibly important is, is go ahead and prepare for an incident. There likely will be one, it, it may not be one that puts you on the front page of the newspaper or has news vans rolling up.

Courtney Doyle (12:06):

Hopefully Yeah. <laugh>,

Patrick Kelley (12:07):

Hopefully, you know, but at the end of the day, more than likely you're going to have an event. So having an instant response plan that has like playbooks built in, because here's, here's something crazy, no matter how well trained, um, boards and companies are that I work with that have a good instant response plan when ransomware hits or when someone has gained access to something, you know, unauthorized, it's really hard to get past your emotion. The whole world's on fire. I'm gonna lose my job. I may lose my whole career. Know what are we gonna do? Having, you know, a playbook that has next steps written out of it. It gives you enough time to, to walk through the first four or five hours, and that's going to do a couple things. Um, and four or five hours is probably going to become apparent that things are going to be okay.

Patrick Kelley (13:08):

It's going to be uncomfortable. Um, it's going to be stressful, but no one's gonna die. Um, we're gonna get through the other side, you know, we're, it, it's going to be okay. The other is that you're gonna have a chance to figure out exactly what has gone on or at least have a pretty good idea of what's happened. So is playback really help? And in those, for listening to the podcast, if you don't have an incident response plan with playback, send me an email or send it through Cherry Lynn and I will give you a free incident response plan with playback built out. It's a template, but it's a really good one. Um, it's a really good one, <laugh>. So, um, even if you just find and replace names, you'll have something.

Courtney Doyle (13:54):

Oh, that's amazing. And then

Patrick Kelley (13:55):

Most importantly, from a technology point of view, it's just patch. What most of the breaches that we're seeing in the energy space is truly comes down to just poor hygiene. Just, just patch. Mm-Hmm.

Courtney Doyle (14:06):

<affirmative> They find the holes, essentially.

Patrick Kelley (14:09):

They

Courtney Doyle (14:09):

Will. Yeah. Well, can you talk us through a little bit? I'm, I'm glad you talked a little deeper about the, the incident response plan. Um, 'cause I know that's been a big focus of our here over the past several months, is really shoring up that plan. I know in the co-op world, we like to share everything. We wanna say, oh, we found this successful, we wanna give it to you. But at the same time, with cybersecurity, there's a, there's a level of not sharing and that's a little foreign to us. <laugh>.

Patrick Kelley (14:37):

Yes.

Courtney Doyle (14:38):

<laugh>. So, uh, because, you know, we're used to, we, we were successful here. We want you to be successful here as well. Um, is there, I know you said you have a template. Do you have any tips for getting that ball rolling? Because it is really intimidating for people who don't have that or haven't started it and, and you do one and you're like, this is awful, we gotta start over. Or it's just kind of a huge undertaking.

Patrick Kelley (15:04):

It is. It, and I think my advice is, is largely in, in my action of take a template, you know, something that is at least framed up when you, when you've never written an incident response plan, and you just sit down in, in your, you have the enormity of, of what that is like right in front of you. You know, what systems do I have? Who do I contact? Where do I put that in here? It needs playbooks for a ransomware attack or for a business email compromise. Maybe you've never been through one of those, so, you know, what, what steps, you know, do you write down for something that you've never been through? Mm-Hmm. <affirmative>, you know, one of the, one of the interesting things that I was, I was shared as a, as a, as a younger kid, you know, I think I was 12, maybe 13 at the time, is my, uh, my bonus stats. One of the hardest things I ever did in my life is, is my professor tasked me with writing a paper about nothing. And it had to be 10,000 words about on the topic of nothing.

Courtney Doyle (16:15):

That's what, that's what writing your first SERP feels like. <laugh>.

Patrick Kelley (16:19):

Exactly. Um, how, how, how do you quantify nothing? Well, how do you, how do you quantify the enormity of everything? So I think even if you don't share it, you know, starting with a template is fine. Um, one organization getting through a ransomware event is quite similar actually to another, you know, there is a compromise. We have to determine who gained access. We have to determine what they gained access to. We have to determine if we're gonna call the insurance. We have to determine if it's covered by, you know, if we can cover payroll. There, there are a lot of these things that are incredibly important. Um, but if you choose to go to route of writing your own, the things that I, some tips that I would recommend, recommend in particular are don't call the insurance company first. Um, don't call the federal government first.

Patrick Kelley (17:15):

Don't even call your cybersecurity company necessarily first. I, I tend to recommend calling an attorney. Um, you may wanna call the attorney and the cybersecurity person at the same time and, and have it on a bridge call. But the attorney is going to tell you what your responsibilities are. You know, what your liabilities are and what you know, maybe what you need to do as it, as it pertains to current regulatory compliance. The second, second step is still not call the insurance federal government. The second step is to make sure that you're gonna make payroll. If the company couldn't defend itself with the resources that it had from a ransomware event, it won't be able to recover from a ransomware event while continuing to operate as a company. So if people are afraid that they're not gonna get paid, they're gonna leave you. Additionally, don't want people going to social media and giving their hot take on what's going on at the EMC because chances are it's gonna be wrong, but you're going to have to defend it.

Patrick Kelley (18:25):

So making certain that, you know, call a DP or you call whoever's handling your, your payroll and, you know, call Proline or similar and say, Hey, you know, are we gonna make payroll? And if you are, then you call, you know, DHS or the FBI or Secret Service. That's when those people come into play and you call the insurance company. But, but you always start with, as an organization, legally, what are we supposed to do here? Number two, will our employees be paid on time? Will there be a disrupt in? How do we get around that Three, let's look at calling in, um, the FBI secret Service Homeland. 'cause they're gonna be able to help you quite a great deal. And then you have to determine are we gonna call the insurance company or not? That's very different than what most are gonna tell you. You know, call the cyber company, call the FB, I don't do that.

Courtney Doyle (19:23):

Yeah, no, I'm, I'm, I'm surprised too. So that was, um, I'm sure Steve knows that <laugh>, so I'm sure Steve will just be disappointed in me that I'm surprised. But, uh, it, it's probably

Patrick Kelley (19:34):

I get a lot of wide eyes when I say that in. Yeah.

Courtney Doyle (19:37):

Well,

Patrick Kelley (19:37):

And then when I, when I walk through the reasons why they're like, okay, you know, that, that, that makes sense now.

Courtney Doyle (19:44):

Yeah. A little shock value up front. <laugh>

Patrick Kelley (19:46):

<laugh>. Right.

Courtney Doyle (19:48):

So I wanna switch gears just a little bit and talk more about just some real life scenarios that maybe you've seen in the utility space and some things that, you know, we should be aware of other co-ops should be aware of and, um, kind of what the result was.

Patrick Kelley (20:09):

Sure. So, you know, I think that's going on and, and I can use a case study, for example. Um, we had an EMC that deployed some fairly traditional tools into the environment. They had a vendor that came in and helped them do it, and then the vendor left. And, you know, the EMC could afford, uh, you know, to pay for some contracting hours, but, but not for long-term support. So there was a platform of tools that, that, that was rolled out in the environment, and they were configured in a particular way. What ended up happening is that, that those things weren't patched. Um, the EMC, the co-op did not know that they had to be patched. They just knew that they got reports from them once a day. What ended up happening is, is that third party vendor in that toolkit was compromised, which led to a full compromise of that EMC in the co-op that led to, um, some very close calls into a few of the substations in remote offices because they were starting to do smart grid, smart meters, um, and, uh, fiber optic connection.

Patrick Kelley (21:18):

Yeah. They started connecting everything. And when you start connecting things, you, you tend to connect them with faults, you know, default settings, default credentials, things like that. So, moving around the network was very easy. This threat actor lived there for about six months when we went back and, and, and did the investigation and triage, the, the mc and co-op never knew. And the lessons to learn, you know, from that, and it starts playing forward, is you have to know what you have in your environment. Like, there, there's, there's a really good phrase. You need to know what you have to protect, and you also need to remove things that, that you don't require, you know, in your organization, like maybe the extra servers or data, because you also don't have to protect what you don't have. So if you're not scrambling around trying to protect things that don't have any business utility, then you can focus those efforts elsewhere where you need to.

Patrick Kelley (22:14):

And when you do a, when you do, you know, some sort of inventory or, or asset collection, you'll learn about these systems that are laying around in your network that maybe you didn't know about. And those sort of things that typically get you breached. If I draw a quick correlation against governments, a lot of your city, county, and state governments get breached through systems that they themselves did not put in their networks. It was vendors that came in that did a one-time contract that deployed a functionality that the EMC or co-op or government needed, and then they left. There wasn't a transition of knowledge or skills, you know, to the, to the existing team. So they didn't know what to do with it.

Courtney Doyle (22:55):

It's more and more sounding like, you know, the, it just really paints a picture of the value of having a team member who is dedicated to this space, who can be the expert on these things, who can spend the time getting to know every single vendor that touches every corner of the organization. And then finding the overlaps. And it just 'cause it just feels like a, a constant job, right? You're never just done, as soon as you're done doing the audit, you gotta start over and do the audit again. 'cause it may have been a year or something like that.

Patrick Kelley (23:28):

Yeah. There's, there's, to build on the, on that point, there's, there's two very important things I think that we miss. And it's, there needs to be a cybersecurity person, but who does that cybersecurity person report to? Mm-Hmm. <affirmative>. Is it a chief risk officer? Is it the CFO? Um, it, the security person diff typically does not need to report to the CTO. Um, the reason why, and, and this might catch a few people off guard too, is that even though cyber security has technical components mm-Hmm. <affirmative>, it's actually more, um, risk and, and policy driven. IT and cybersecurity also are competing mission, and I'll break it down a little bit. You know, the IT person is most concerned with availability, like email has to be available. Mm-Hmm. <affirmative>, uh, the payment system has to be available and they will just about sacrifice everything for availability. The cybersecurity person, on the other hand, has a focus on risk, like it can be available so long as we're not bringing, you know, unacceptable risk to the organization. Mm-Hmm. <affirmative>. And that ties into one last nugget to that, which is every organization has risk

Courtney Doyle (24:49):

Inherently. Yeah. <laugh>.

Patrick Kelley (24:51):

And you can't, you can't have an organization without risk. I like to go to the beach and get in the human sling shot. It's one of my favorite things to do. <laugh>. I love it. It's exhilarating. The view is incredible. I love the human slingshot. It's not the most secure thing that you could do. And I'm a security person. And the point of that is that I, I'm not telling organizations not to take on risk. I ask organizations to understand the risk that they're accepting. Mm-Hmm. <affirmative>, I understand when I get a human slingshot that I'm accepting some risk

Courtney Doyle (25:25):

That you may end up on the moon and I'm willing

Patrick Kelley (25:27):

<laugh> right at, you know, or right out there in the middle of someone's sandcastle. You never can tell, you know, once you're on for the ride, but as long as you, as long as I understand that this is the risk I'm accepting, then all's fair.

Courtney Doyle (25:44):

Yeah. All of a sudden you're more prepared for it because you have acknowledged what that risk is.

Patrick Kelley (25:49):

It may, it may come with a, with an unplanned dismount, um, <laugh>, but I, but I had an idea that it was coping <laugh>.

Courtney Doyle (26:00):

Yeah. Well, I wanna get two more quick questions then before we let you go. Um, one is, and we kind of talked about it at the very beginning, how cybersecurity is changing all the time. Technology is changing all the time. I feel like for a long time we heard about ransomware and data breaches, but now we're hearing a lot about like AI and deep fakes and all that kind of stuff. So what, any thoughts on what's next for this realm as far as all these new technologies and managing the risks that come with those new technologies, especially as fast as they're coming?

Patrick Kelley (26:35):

Yeah, I, so I think that that's a great question. And it has, it has an interesting place in utilities. Um, I don't think that how access to utility networks is going to change greatly. Um, I think the basics are still going to be the, the main thing. You know, patching, having two factor authentication, things like that. I think that's very important. I think it's good. What's going to change is the velocity and what comes after, you know, a breach takes place. I feel like with AI and machine learning that breaches are going to happen a lot faster, um, than they have in the past. I think we're seeing that right now. There's an interesting question post in a conference house at yesterday, which was we decided not to pay the ransom, and the ransomware group didn't post our data <laugh>, and we never heard from them again what's going on.

Patrick Kelley (27:34):

And we said, well, with AI and machine learning, they're, they're able to gain access to more victims than they ever had before. So they're managing their portfolio. We don't have enough attention for this little company over here because we're currently working with an oil company like Colonial, or we're dealing with a larger target. So they just, they walk away because they already have plentiful targets. But the story doesn't stop there. The EMC and the CO because there's no closure. So I think we're gonna have a higher velocity of it happening. Here's what I think is gonna happen next. I don't think that ransomware as, as the way we see it today with encryption and, and removing access to things is going to be the norm. There are two very important components that come to, or, or three in fact that come to data, confidentiality, integrity, and availability.

Patrick Kelley (28:33):

Right now, ransomware and deploying encryption has been about availability. It's been this way for a while. We're going to encrypt all the data, and if you don't have good backups, then you won't be able to get to it and you're gonna pay us money over the last five, six years. Most orgs do really good backups now, or, or a lot better than they did. And the threat actors know this. So they've moved to, let's just take the data off the network and let's attack the confidentiality of it. That's what we're seeing in healthcare. Not even worry about taking it offline. The value of the data's confidentiality is much higher than the value of its availability because they have backups. So you're gonna see more of that. I think Office 365, Google Workspace, a DP, things like that are gonna become bigger targets because we don't have to worry about getting around the firewall. You know, the attacker can just log into Office 365, download everything from SharePoint in OneDrive, and the confidentiality of the data and the value of that confidentiality is what they can bargain with. So we're gonna see more of that. So it's gonna be higher velocity and, you know, what happens with that data on the other side,

Courtney Doyle (29:44):

Is there anything that we should be talking to our members about that they can do to help us? You know, we're doing everything we can on this side to keep all of our stuff secure. Is there anything that our members can do? Because I think of, like, we have Smart Hub, it's a portal where our members can log in and, and see their information and manage their accounts and things. You know, what can we do to best educate our membership so that they can help us on our mission to keeping everything safe and secure?

Patrick Kelley (30:15):

Sure. Um, I think there's three primary things that I would have an individual or, or a member of a co-op fo focus on. One is understanding that all data is likely to be breached if you put it on the internet, whether it's Facebook or, or, or whatever you choose. So be mindful in the data that you share. You know, if we're looking at 23 and me right now, there's a great deal of DNA and, and very sensitive information that was put there. And the future of 23 of me is very uncertain. So you have to be very mindful about what you're sharing. Um, number two, I'm a big fan of a password manager. You know, if I'm using the same password for Facebook as I'm using for the portal that I have at cherryland and my Facebook account is breached, then my Cherryland portal account is breached as well.

Patrick Kelley (31:02):

These are, these are very one in one things. So a password manager, and they're free by the way, you know, for an individual like LastPass one password, these are free things. You do not have to pay for them. Um, it will recommend unique passwords for each one of these things, which will help you because if Facebook is breached, you're my portal or your portal for Cherry land won't be, uh, the last thing is two-factor authentication. And it's probably the most important of the things. Even if an attacker has your username, the password, you know, if it has to have your phone or it has to know some se second factor of validation that you are who you are, they're typically not going to be able to compromise that account. So, you know, even it, it being a text message or using an, you know, an app that you get from Google or from your bank or something, you know, that second factor of authentication. So to wrap things up, you know, what are you sharing? Do you really need to, um, password manager so you're not reusing them and a second factor of authentication in case that password does get breached.

Courtney Doyle (32:06):

That is super helpful and great reminders and things that we certainly will, uh, continue to share with our members as well as we're, we're trying to share as much as we can about what we're doing cybersecurity wise to hopefully instill some confidence in the members about what we are working towards. But like we said, a lot of it is sensitive, right? So we keep a lot of it also under lock and key, but I just, uh, hope

Patrick Kelley (32:31):

You're <laugh> I'll say you're a very rare organization,

Courtney Doyle (32:35):

Really.

Patrick Kelley (32:37):

I, yes. There, there are very few EMCs that are educating their members on, on the challenges of cybersecurity. Very, very few out of the, out of the 900 and some odd I think that are in the United States, you would definitely be like in the one or 2%. So I'm very proud of your mission. When, when the message came over about, about doing this interview, I was like, wow, this, this is refreshing and odd. <laugh> and, and

Courtney Doyle (33:08):

<laugh>. I'm glad we could give you that feeling. I'm

Patrick Kelley (33:11):

<laugh> it's, it, it was just, it, it's very, I'm invited to do conferences, you know, where I'm in, in front of a lot of people, but they're generally put together by these large consortiums that have federal dollars. Mm-Hmm. <affirmative> that, that's almost compelling them to do it. Mm-Hmm. <affirmative> and EMC or, you know, cherry land coming out saying, Hey, we want to do this, and by the way, we wanna have some of this focus on our members, not normal. Um, so I, I definitely applaud y'all for, you know, going above and beyond to do this sort of thing for your members. It, it does actually show a lot.

Courtney Doyle (33:44):

Well, thank you. We're, we're extremely fortunate to have a really supportive membership, a really supportive board who allows us to invest in things like cybersecurity. And like I said, uh, Steve, uh, he's our cybersecurity administrator. He is awesome. He is, he is so focused on this. Like I said earlier, when I asked him, I said, Hey, who should I talk to? And he was like, I know just the guy and emailed you. And then within five minutes we were in touch. So, so, um, we were Appreciate it.

Patrick Kelley (34:11):

<laugh>. I have to compliment Steve. I I did, I have found him the couple times I've met him and, and we've spoken through an email in, in LinkedIn. He is, he is an, he is an exceptional <inaudible> security person, but thus far in as example of of, of what we need in EMCs and co-ops. I, I just find him to be just an accept exceptional example of, of what that should be.

Courtney Doyle (34:35):

We are so grateful and fortunate to have him working on behalf of our members, uh, to keep everybody, keep all of us safe in the, in the cyber realm. So. Well, thank you so much Patrick. We really appreciate your time. Well,

Patrick Kelley (34:49):
Thank you.

Courtney Doyle (34:50):
Thanks for listening. Be sure to join us next time for more co-op Energy Talk.