Stephen let's start with you. Would you explain to various layers of substation physical security and why it's such an important consideration?

Stephen Dulin (01:43):

Sure, Nadia. Thank you very much. Um, I just wanna start off by, uh, reiterating the importance of the substation physical security program. Recently, there have been several substation attacks in multiple states leading to long customer outages and costly repairs. Um, we've seen a lot of that here in the news not only in the past couple of years but really the past five to 10 years.

(02:05):

So we have been proactive in increasing the physical security measures of our stations throughout Virginia to hopefully mitigate these adverse security events as well as improve reliability to our customers. So I can't dive too deeply into the various different levels of our physi- physical security upgrades, but we are completely renovating the security, s-, uh, renovating the security measures at all the stations that we have selected for the program.

(02:32):

And some of the upgrades, um, that you will see include taller fences as well as stronger fences, which will hopefully keep, uh, vehicles from running off the road and going through the fences, as well as keep residents in surrounding areas safe, uh, and their children safe from, you know, entering the substation.

(02:50):

Also included is innovative monitoragy... Monitoring technology. And these improvements will greatly improve the security at the substations. And I can't get too... Into too much depth on to what those entail, but they are innovative and will help greatly in keeping our substations secure, uh, moving forward.

Nadia Ely (03:19):

Great points, Stephen. Thank you. Turning to you now, Sean, Corporate Intelligence and Security utilizes a converged security model which puts both physical and cybersecurity into the same department. Sean, could you explain how that model benefits substation security?

Sean Stalzer (03:37):

Sure. But let's first go back a little bit in time, and just let's discuss converged security. So five years ago, um, there was no such thing as converged security. And, in fact, at Dominion Energy, we had the physical security group, and they had an operation center, and it was located in the basement of OJRP, which still existed at the time. We had a cybersecurity operation center, 14th floor of Eighth and Main downtown. "Never the two should talk because why should physical and cyber have to talk? That doesn't make any sense."

(04:01):

Fortunately, Rodney Blevins had the vision. And he had the vision that, "Hey, these two groups are gonna need to talk. The threats are evolving." And as we started building the Farrell Building, he kinda sketched out what, what the fifth floor should look like and how those groups should come together. He hired Adam Lee, who was our first chief security officer and came to us from the Richmond FBI office, where he was the special agent in charge.

(04:21):

So we started there with, "All right. Now, we're, we're the power company of the Pentagon. We have a huge percentage of the internet's data centers. We, we are the headquarters to many of the three-letter agencies. And there's all these risks emerging. We need to converge the two security groups so they operate as a single entity." If you think about how the risks going forward are gonna look, they're anything from radical dome- domestic groups, disgruntled people, criminal actors, and definitely nation-states like China and Russia that I'll touch on in a later question.

(04:48):

But in the event there's a major shooting war or, heaven forbid, you know, Russia gets angry over Ukraine, or China decides to invade Taiwan, the prevailing thought process behind the government is, "That will be a combined cyber and physical attack on the energy infrastructure of the United States as part of the opening salvo."

(05:05):

So we put this converged security model in place with that idea that future threats are going to have to be solved simultaneously physically and cyberly. The more walls and barriers there are in between making that happen, the longer that takes. Homeland Security came down. They did a study. They wrote a whitepaper. They name a large East Coast utility, meaning us. In that paper, they said, "This is the way you need to run a security organization."

(05:30):

We dubbed our, our group the TRAC, the Threat, Response, and Analysis Center, which is the fifth floor. And if you were to come down there and take a tour, you would notice that what used to be two separate buildings, "Never the two should talk," is now one contiguous room. They share overlap on their telemetry walls. The managers meet and talk.

(05:47):

So in essence, the answer to your core question, "How does that benefit substation security?" well, when you have your physical and your cyber groups, they're training together, they're working together, they're fighting those daily battles together, they really are an integrated team, then in the event Stephen and crew have an issue that pops up, either we're gonna see it sooner, or we're gonna be able to re- react to it more efficiently and effectively than we ever could in the past or that we ever could with diverge separate groups.

Nadia Ely (06:20):

Thank you for the background and the thorough answer, Sean. I appreciate that. This next question has two parts and is directed to you both. So, Stephen, what challenges does your team face when implementing the security standards that Sean outlined? And Sean, can you talk about how Dominion Energy stays current on the threats posed to our critical infrastructure and what some of those threats might be? Stephen, I'll start with you.

Stephen Dulin (06:45):

Sure. Uh, like most large construction projects, there's always gonna be challenges to work through during the different construction phases. Most of our projects will require, uh, several environmental and municipal permits, uh, amongst other different types of permits, just in order to complete the construction. So the permitting phase itself can significantly impact a project's schedule and budget. So that's one of the large items that we've, we've been, uh, working with on these projects.

(07:13):

And on several of the projects, we've actually had to extend the footprint of the substation, which also leads to additional challenges. Um, in the eastern part of the state, for example, the water table has actually presented an unusual challenge. While we've been trying to install a new, uh, fence post on these projects, we've had to actually bring in special equipment in order to set the poles at these locations because the water table would actually force the poles up out of the ground, and we can't get them to, to set firmly in place.

(07:41):

So that's, uh, something that, uh, we've definitely had to fight through on, on several of these projects. Uh, so it really takes a great deal of communication between the different parties in order to successfully complete all these projects in the field.

Sean Stalzer (07:58):

So on the topic of how do we stay current on threats to help better inform those construction projects or even after they're live how we makes sure we're protecting things, a d-... A core mission of our department, which is CIS, Corporate Intelligence and Security, that's that combined physical/cyber threat intelligence bubble here at Dominion, a core mission of that is developing and maintaining deep government relationships.

(08:19):

And by that, I mean relationships with FBI, Homeland Security, you know, CISA department or Intelligence and Analysis Department, the CIA, NSA, Department of Defense, like the Marines, as example, or the, or the National Guard, they have a cyber brigade, Department of Energy.

(08:34):

So we have a whole focus on maintain those relationships. Then when you have those relationships, and you have security clearances on key individuals, then they're much more likely to talk to you, and you're much more likely to learn things. You're gonna stay current on what's going on in the world. What, what we see in the news is never the whole story, and it's often missing critical pieces and components, and it's often way late. By the time you hear about something in the news, as a good example, um, it's long since been exploited in the wild.

(09:00):

China and Russia can scan the entire internet within 30 minutes. So that means by the time it makes it news story, even if it makes it the same day, hours of cyber attacks could've gone on. And so we stay very current by having those government relationships, but that's a two-way street. When I first got this job, I was convinced, right, "The government can see everything," you know, this giant conspiracy theory that, "They know everything that's going on and every email you send." In reality, they don't know a whole lot unless we share. So there's a bidirectional sharing going on.

(09:27):

For example, I talk to them about who's attacking our perimeter and how they're doing it, and they share back with us sort of tactics and techniques that are being used, things we'd wanna block, bad actors that are emerging. We have Homeland Security as a part of our team. They are virtually inside of the top Farrell Building, so to speak, watching our network traffic to help protect us against classified information.

(09:49):

I have a full-time US Marine that's paid for by the US Marines who sits inside my SOC on the fifth floor, and, and he, soon to become she, um, as we swap out one bringing for the other, their, their whole job is interfacing with Department of Defense in helping to keep us safe. The FBI gets a dump of data every month from us. They return a whole bunch of great stuff to us.

(10:09):

So really, it was an entire effort around not just being really, really good at cybersecurity but gaining that intelligence and insight from the government so that we can be better at it but also providing them information to make threats go away. You know, we are... We, as a private company, can't take offensive action. We can only defend. And so we... If we give them the information, they can arrest people, as an example, and make threats go away.

Nadia Ely (10:35):

It's fascinating to see, Sean and Stephen, how all the pieces fit together. Thank you. And sticking with you, Sean, how does the cyber team support other business segments, like Grid Resiliency, to ensure our strict cybersecurity protocols are implemented properly?

Sean Stalzer (10:53):

Sure. So I think for a lot of years, if you had asked anybody at, at Dominion or really any big utility, "What's cybersecurity?" you'd hear, "Well, you know, that's, that's NERC CIP. That's those NERC regulations." Well, regulations are compliance. While they have a secum... Security component built into them, compliance isn't security. Compliance is primarily paperwork.

(11:13):

So Dominion recognized that back in about 2019, and instead, we internally developed what we call our minimum cybersecurity standards. Um, and that's... Applies to all operational technology areas. That could be everything from facilities things, like the lights and the heating of our buildings, all the way up to nuclear reactors and substations and power generation plants and offshore wind, and you name it, it applies to it.

(11:35):

So we have a team within my cyber organization who are engineers, right? They came from the business area. Uh, they are very smart on the business side and very smart on the cyber side. And there's a team on the physical security side. And together, they work with those business segments to have the kind of discussions that Stephen was talking about earlier, the, "What are the right controls for a substation? How tall should that fence be?" as an example. Or, "What kind of structure, what kind of material should it be made out of based on what kind of threat we are trying to mitigate for that area based on how important something is?"

(12:07):

But I think a key thing for all of that process of, of keeping current is that, "Whatever we do today, is it good enough for tomorrow?" So we are constantly learning, constantly innovating, constantly updating our standards and our processes. A good example is artificial intelligence wasn't even a thought process two years ago even, even a year and a half ago, has really emerged on the scenes lately.

(12:28):

And that's because your bad actors, like your Chinas, your Russias, even your environmental groups, et cetera, they don't go, "Ah, you stopped me. I give up." Right? They're smart people. They iterate. They come up with a new way to attack. So we've gotta be smarter than they are and constantly be updating our defenses.

Nadia Ely (12:49):

It's funny, Sean. The average person doesn't realize how many threats per day, uh, we are actually facing, so, uh, thanks to you and your team for all that you do. So for the last question, I'd like to... You to both to weigh in. Uh, how do you see these physical and cybersecurity standards protecting our company as well as our customers? Stephen, I'll start with you.

Stephen Dulin (13:10):

Sure, Nadia. I'll just say that these projects are vital to ensure, uh, we can mitigate adverse events from occurring at our substation locations. And ultimately, this will help keep our residents safe as well as improve the electrical s-... Reliability to, uh, the customers that we serve.

Sean Stalzer (13:31):

And I'd add to what Stephen was saying, in terms of what you just mentioned, Nadia, about not everybody really understanding sort of the threat that we face, one of the things that we offer out of my group is what's called the Cyber Threat Briefing that one of my managers, Mark Shalowitz, and I give. We've talked to over 14,000 employees and contractors so far.

(13:47):

And because of that, that same point you just made, I start every single presentation by saying, "We are at war." Uh, and I don't think a lot of people understand that the United States is literally in a cyber war with China and Russia all day, every day, all across the country, whether it's trying to bring down the grid, and that's a huge focus of China and Russia, is to build the tools to crash the grid, to steal property, to steal information.

(14:10):

Um, to lesser extents, you get Iran and North Korea playing in there. North Korea likes to steal money, for example. They don't have a very big budget, so they like to steal money in any way they can do that, for example impersonating a vendor and getting us to pay a false invoice. There's all kinds of threats to the grid that are going on out there.

(14:24):

When you look at the United States, the government considers the energy sector the single most critical sector because, without power, nothing else works. And they consider Dominion Energy the most critical of all energy companies. So, as a result, we operate sort of on a war footing every day. We are fighting nation-states all day, every day, to keep them out of the grid and, and away from these substations, as an example.

(14:47):

So, overall, you say, "How do these standards protect us?" Well, by having these standards, by having strong government relationships, by having great partnerships with the business area, and then by taking advantages of things like the Grid Transformation plan, we can basically add strong controls and update those controls over time, and then be ready, should the worst ever happen, to respond in a timely manner and restore service, both electrical service as well as cyber and physical connectivity, to those locations.

Sean Stalzer (15:35):

I think the only point I would drive home is, is simply the idea that cybersecurity or even physical security of any location is really not just the responsibility of Stephen's team or the CIS department. Every employee plays a role, whether that's paying attention to an email that comes in and not clicking on a link, whether it's not letting somebody tailgate in behind you, whether it's, "See something, say something." If anything looks off to you in the physical space, the cyberspace... You drive by a substation, and there's a tree down on a, on a fence or something... If you see something, definitely say something.

(16:06):

And if you're not... If, if you don't know which place to go and have it reported, I think it's 1-800-DOM-TRAC is our number, right? And that, that takes you right into the physical operation center on the fifth floor here, and they'll route it to the correct people. But the point is we all play a role in it. Security is part of everybody. Keeping the, the grid up and running is something that all of us should be a part of.