The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Transcript

Part 1: Public Private Partnership Essential to Develop ES-C2M2 in Five Months

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Division is part of the Software Engineering Institute. We are a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a principal researcher at CERT working on operational resilience. I am very pleased today to welcome Jason Christopher with the U.S. Department of Energy (DOE). Jason is the Technical Lead for Cybersecurity Capabilities and Risk Management. And I'm also very happy to welcome back my colleague Nader Mehravari. Nader is a member of CERT's Cyber Risk Management team.

And today, we're going to be discussing a topic that I've been trying to get on the podcast series for a long time because it's just such a great topic to let you all know about. We'll be talking about the Electricity Subsector Cybersecurity Capability Maturity Model. It was published by Jason's organization, the U.S. Department of Energy, in May of 2012 and has been in active use since that time.

And just for our listeners' information, CERT did serve as the model architect with DOE for this effort. So, Jason, welcome to the podcast series. We're so happy to have you today.

Jason Christopher: Thank you very much. I'm glad that I could be part. I'm looking forward to having a discussion.

Julia Allen: And thanks for coming back and participating with us, Nader -- appreciate it.

Nader Mehravari: Hello, Julia. I'm delighted to be back on the podcast series. Thank you.

Julia Allen: So, Jason, why don't you set the stage particularly for our listeners who aren't that familiar with this body of work? So, what is the Electricity Subsector Cybersecurity Capability Maturity Model -- Doesn’t quite roll off your tongue -- we call it ES-C2M2, and a little bit about the catalyst for its development? Could you fill us in?

Jason Christopher: Certainly, I'll actually start off by saying the Department of Energy has been really active in cybersecurity for the energy sector for many, many years. We actually started off in 2006 with a roadmap for controls in cybersecurity.

That has now been evolved into an update in 2011. And this effort aligns with those. So, this is nothing that has come out of the blue or anything like that. The model itself is allows electric utilities and grid operators to assess their cybersecurity capabilities, prioritize their actions and investments to improve cybersecurity.

We're looking at four different goals that we were trying to work with through the model. (1) First is strengthening cyber capabilities within the electricity sector. (2) The second is enabling utilities to effectively and consistently evaluate and benchmark cybersecurity capabilities. This is something that we constantly get asked about regarding the model, whether or not -- how am I doing compared to my peers? (3) And the third goal is to share knowledge, best practices, and relevant references within the subsector -- something that's actually a very natural fit for a maturity model. (4)

And lastly, but certainly not least, it is to enable the utilities to prioritize their actions and investments to improve cybersecurity. When you're looking at the model, and we can discuss this a little bit later, you're actually given a scorecard. And the scorecard itself can be leveraged to inform you about where your gaps are and how to achieve on improving those gaps.

Julia Allen: Okay. So, Jason, you mentioned that the onramp for this model was based on work that the DOE started quite a few years prior. Do you recall or were you part of what put cybersecurity on the DOE agenda in the first place? What made them decide that this needed to have some investment in this area?

Jason Christopher: Well, it's always been a national priority. It's something that our sector itself has been dealing with for quite some time. Ever since the blackout in 2003, there are actually mandatory cybersecurity standards that were placed on the sector that are actually managed by the Federal Regulatory Commission.

So, cybersecurity for the sector has been a very important piece of how they do business and how they maintain reliable operations of the grid. These results and work in that has really just been an organic growth from that because a lot of what we do is public private partnerships with those utilities and asset owners.

Julia Allen: Okay. Well, that makes sense. So, can you say a bit about how the model was developed, who some of the key stakeholders and thought leaders were in getting the model to completion?

Jason Christopher: So, we actually started this effort back in January of 2012. And as you said earlier, the result was published in May 2012. So, for a model to be developed in that time period is really something that I think is pretty phenomenal, especially considering it had to be done with private partnership. This was not going to be a big government [??] that was just going to be left on a shelf somewhere. We really wanted to make sure the industry was actively engaged in the process.

So, it was a White House led initiative. It was co-sponsored with DOE and DHS, who worked together with other Federal agencies, and as I said before, asset owners and operators. The whole goal of it was to actually have a model that would be able to help with the idea of how secure is the grid? And so, the model itself would have to be developed and applied to all electricity utilities regardless of their ownership structure, their size, what they do for businesses, what they do for reliability.

So, within that we were able in that five month period to help with not only the development of the model but also with piloting the model with 17 different utilities. So, within five months, we were able to sit down, have workshops to help answer the questions about how secure is the grid, what did that capability maturity model look like, but then also go to utilities, actually vet and validate what we've done and what we've been able to accomplish with that.

Julia Allen: Yeah, I remember what an intense period of time that was for all of the people involved at least as we saw it from the CERT perspective.

I am curious though, with that diverse of a stakeholder base, and with the private public partnerships, how -- I'm just curious -- how did you reconcile the issues between maybe the smaller, more specialized utilities and the larger utilities that have the largest customer base? I would envision that there would be some model issues or some practice issues across that wide range of potential users. So, do you have any anecdotes or examples of how you actually reached consensus?

Jason Christopher: A lot of long nights. It really came down to that, the piloting process. We worked together not only with the utilities themselves but also with the trade associations that represent those utilities.

So those trade associations represent not only the large utilities, but also the small utilities, the munis and the co-ops. So, there's a very diverse pool but there's also a very diverse way of tapping those people and being able to get that collaboration across all utilities. So a lot of long nights, a lot of conversation but that piloting process is also very vital.

Julia Allen: And it sounds like -- just looking at the outcome in the short period of time -- that there was a very high intention of all the participants to actually work to make this happen. Do I have that right?

Jason Christopher: Yes, absolutely. I would say the first, anecdotally, the first couple of workshops there was a lot of dialogue about, "Would this be a new effort? Why do we need a new effort compared to all these other things that we already have?"

As I said before, that was the catalyst for getting those other efforts and putting them into this. So, this wasn't something that was one off and by itself. It was really a common model taking the best practices that we already had as a sector and being able to incorporate it into the model.

Part 2: ES-C2M2 Structure and Self-Assessment Method

Julia Allen: Great. Thank you. So, Nader, I would love to get you involved in this conversation. Can you tell our listeners a little bit about the topics that are covered in the model and its structure?

Nader Mehravari: Sure. To me, the model presents to its users an overarching collection of -- I call them good things that an organization should be doing in order to manage and improve their cybersecurity posture. In other words, it provides a long list of cybersecurity practices.

Now, that list is very long and therefore the model organizes this long list of cybersecurity practices into 10 -- you can think of them as logical groupings that the model refers to at domains. There are 10 domains in the model and each deals with a different subject area.

They range anywhere from some fundamental activities like risk management to some domains that are more operationally focused like asset change and configuration management or access management. And it includes areas that deal with how best to manage all the cybersecurity activities such as workforce management, supply chain, and program management of cybersecurity activities.

So, these are the 10 areas that the (model) primarily deals with. As far as the structure of the model, in addition to these 10 logical groupings, the model provides a set of maturity indicator levels that organizations can use to keep track of their progress, their progress in implementing the cybersecurity practices. There are four maturity indicator levels, MIL 0 through MIL 3. You can think of them as a ruler, a ruler to measure organizations' progress in implementing these cybersecurity practices.

And, in addition to the 10 domains and the 4 maturity indicator levels, the practices in each domain are also organized into groupings called objectives. These objectives are -- you can think of them as achievements that an organization can look for in order to, in support of the domains that these objectives are in.

And maybe I can give you an example. Among the 10 domains, there is one domain that deals with activities dealing with incident response and continuity of operations. That domain is organized into four objectives. (1) The first one is detect cybersecurity events. (2) The second one is escalating more important cybersecurity events. (3) The third one is responding to cybersecurity events. (4) The fourth one is more like a business continuity -- to put a plan in place to continue the operations.

The fifth objective in a domain is dealing with managing all of the above activities. It's a set of common objectives that the model uniquely provides as a mechanism for organizations to determine how they'll have institutionalized the practices that the model provides. So, that's a high level description of how the model is organized.

Julia Allen: So, Nader, would I be correct -- because we work with the model quite a bit -- to say that there's a progression of practices within the domain objectives -- the ones that you said that are specific to incident response and continuity of operations -- but there's also a progression in the last objective you mentioned, the one that's common across all the different domains that talks about how you actually get a domain into organizational use. So, is it fair to say that there's a progression within both of those categories of objectives?

Nader Mehravari: Yes, you're absolutely correct. In fact, we call this a dual progression model, which was one of the unique contributions of the work that the model developers did back in 2012 to provide this type of architecture and put in practice true ES-C2M2. Yes, it is dual progression model.

There are two things that are progressing across maturity indicator levels. The completeness and thoroughness of individual activities are progressing in specific objectives. And also, the extent to which practices are ingrained and are becoming part of the organization's DNA are also progressing and measured by the model.

Julia Allen: Great. That helps clarify and I think draws some distinction with some of the other modeling efforts that the SEI and other organizations have been involved in. So, a model is great. And a model is useful. But unless an organization can actually evaluate or assess itself against the model, it's very difficult to get it into active use.

So, I know that the DOE and CERT team and others have developed a method against which an electric utility can evaluate its performance against the model. Can you tell us a little bit about that?

Nader Mehravari: So, the most important thing to recall about this self-assessment is its purpose. The purpose of the self-assessments are for utilities to assess their cybersecurity capabilities, so they can identify gaps, so they can determine what's the best way to invest their scarce resources. So, assessment is known to identify these gaps.

So, Department of Energy provides a set of resources and tools for utilities to use in order to do their self-assessments. These resources, I would say, fall into two categories. There are a set of instructions, toolkits, pieces of software that are provided by Department of Energy free of charge that utilities can utilize to do the mechanics of the self-evaluation.

In addition, utilities can request Department of Energy to provide expertise in the sense of individuals who are familiar with the model, who are experts in doing self-assessments, and people who can utilize the software and the tools.

The engagement is typically a day long, starts by making sure individuals who have day-to-day operational responsibility in that utility are present in the self-evaluation workshop. The software tools that DOE provides are used by the facilitator of the self-evaluation. As a collective, they go through all the 10 domains, through all the practices.

Questions are asked. Members of the operational activities of the utility provide answers in a sense of, “Are these practices that are being implemented, how well are they being implemented, are they being implemented fully or partially?” And these answers are recorded in the toolkit that are provided by DOE. And at the end of the day, the answers are processed by the toolkit.

And a very succinct and interesting summary dashboard graphically is provided that the organization can use to identify the gaps and then take the following steps and putting in plan to close some of the gaps.

Part 3: Field Experiences and Future Plans

Julia Allen: Okay. And Jason, I'm curious. What, in your experience in conducting these self-evaluations, the ones that you and other DOE folks have participated in, what is the experience? What is it like being in the room?

Jason Christopher: Well, it's actually really interesting. I think that one of the key values of the model beyond being able to list best practices and have people sit down and actually answer these questions is actually the dialogue that takes place.

As Nader discussed, we have these 10 domains. And when we go down -- in order to be able to do this in one day, it's very important that somebody can speak to each of those 10 domains at an operational level. So, you have people in there who are doing the actual industrial control systems operations sitting next to HR people sitting next to people who are actually in charge of the cybersecurity program.

And the dialogue they have as a result, I think, is actually almost as valuable, if not more valuable, than some of the things that are in the model that you're talking about for practices. That dialogue actually tends to help with that institutionalization, that culture of security almost gets a kick start just in the very beginning of the dialogue for the one day evaluation. Really important to see that cross dialogue and the model does a fantastic job of doing that.

Julia Allen: It occurs to me, as you said, the dialogue that takes place is invaluable because I would imagine that these folks typically don't get this kind of time together, certainly not a whole day, correct?

Jason Christopher: Correct, and it's really interesting because you'll have people who will say, “We absolutely do that practice.” And then somebody 10 seats down says, “I don't think we do.”

And to have that dialogue take place and not only see that maybe they didn't have the culture they thought they did or they weren't doing the practices that they were, but even within their different silos, they're doing different things. So, it's really trying to get an organizational benchmark before we can even talk about things that other people in the sector are doing.

Julia Allen: Got it. And Nader, your experiences, is there anything that you'd like to add about your observations during the self-evaluation process?

Nader Mehravari: Some of the more interesting observations that I recall from the sessions that I've been personally present is the benefit that the organization receives during that day itself. Even before we're done with the day's activities, I've noticed many times that the teams who are in the session during the breaks take some time and they realize, “Oh, we've never thought about this. We've never observed this.” So, it's very interesting to see immediate benefits that the Organization -- that members of the organization receive by going through the process.

Julia Allen: Excellent. So, Jason, I'd like to turn this back to you. We've talked a little bit about the objectives, and the model, and the structure. And of course, it's all freely available on the DOE website.

But before I let you go, I'd really like to have you talk a little bit about this journey leading to what some near-term plans might be, how you see the model evolving, how you intend, and your organization at DOE to use it as well as the utility communities. Can you say a little bit about where you see this all going in the future?

Jason Christopher: Absolutely. So, right now I think one of the more important things that I can do for the model is to actually keep it stable. The model itself has gotten, as we've been discussing, a lot of air time with utilities. A lot of companies even outside of the electricity subsector have really enjoyed using the model. As a matter of fact, later this month I'm actually -- we're working on the release of the oil and natural gas subsector version of the C2M2.

We did a very similar process where we piloted with oil and natural gas companies the C2M2 to see, “Well does this fit? Does this work for you?” And we tailored certain things to be able to allow the model to proliferate through yet another subsector. So, the entire energy sector will be having a single tool that they can use with their own tailored differences as a result.

Beyond the oil and natural gas subsector, we're also keeping a keen eye on the NIST (cybersecurity) framework that is being developed as part of the Executive Order 13636 for cybersecurity for critical infrastructure.

The reasons for that -- one of the objectives (I listed the four out before) -- I would actually really love for 2014 to be looking at a fifth objective, which is a way that the C2M2 can help support that framework -- the way that utilities who are only using this model can continue to use the model to meet the objectives of either the framework itself or the voluntary program that's attached to the Executive Order. So, we're working pretty diligently on that.

So, beyond that, I'm going to be continuing with these facilitations. We'll also be working on a facilitator's guide. With over 1300 utilities in the United States, it would probably be very impractical to assume I could go to every single one of them to for C2M2 evaluation. So, we're working on a guide so that anybody could be able to pick this up. The facilitator themselves would have the knowledge needed for the day of the activity. One of the things that I think is really powerful about the model is that nobody else but the facilitator needs to know about the model. As long as you have the expertise as to what it is that you do, you do not necessarily have to read the model, though I would encourage everybody to go ahead and read it. If you just show up for that one-day facilitation, you should be able to participate and get those answers that would help you with the prioritization of investments and things like that through your own cybersecurity program.

So, because the model is so useful the way it is now, I'm really looking at keeping it stable for the next year or so. I would like to get the working group back together again to look at some improvements that we know should be made. But for the most part, we're looking at really just continuing with the sector and making sure that everyone is participating as they see fit.

Julia Allen: Great, great. So, Jason, you mentioned there's so many utilities and you're working on this facilitator's guide and wanting to keep the model stable through the coming year. Have you observed any instances where a utility has actually gone through a C2M2 evaluation more than once and had the opportunity to compare their results?

Jason Christopher: It's actually something I'm going to be working on this year. We keep all the utilities who participated confidential. We don't share that information. We want to make sure that people are comfortable with information that they're getting, but also that when we go out and facilitate or if they're going to request a toolkit, that is kept with relative sensitivity.

However, there are certain very vocal utilities who have loved working with the model that have actually themselves gone through it internally a few times. But I would like to be able to engage more to see what utilities have done to improve, look at that delta of improvement, and see what that can help the model drive forward in the next coming years.

Julia Allen: Great, great. Because if you might appreciate on the CERT and SEI side of things, we promote and encourage folks to use these models. But the actual ability to measure improvement over time requires organizations to make a commitment to assess, and then put some improvement in place, and then reassess, and then for us to actually see if there's been any true improvement. So, we'll be eagerly watching as you move that part of your initiative forward.

Jason Christopher: Absolutely, as will I.

Julia Allen: Right, right. So, we can all see what kinds of value this type of effort does actually produce.

Jason Christopher: Absolutely.

Julia Allen: Well, as we come to our close, I'd like to give you both an opportunity to point our listeners to some additional references. We've barely scratched the surface in this conversation and hopefully, we've peaked listeners' curiosity about learning more. So, do you have some favorite places, Jason, that you would like to refer our listeners?

Jason Christopher: Definitely the C2M2 website. I'm actually hoping to sort of revamp that website by the end of the month. So, there may be more information for people like the user's guide and other resources that we've talked about here today.

And also the program overview that Tamara Moore, the original lead for the project, gave back in 2012, as well as I believe I mentioned the Executive Order 13636, which is good bedtime reading material for everybody.

Julia Allen: And am I correct that on the ES-C2M2 website, folks can actually get the model and the self-evaluation toolkit that Nader described?

Jason Christopher: For the self-evaluation toolkit, in order to maintain what utilities have received it, we've asked that somebody email us. The email address is on the website but it is really just esc2m2@DOE.gov. So, it's very easy to remember. But the model itself, the PDF, can be freely available online. The toolkit, which is also free, requires an email.

Julia Allen: Great. And Nader are there any other places you'd like to refer our listeners?

Nader Mehravari: I have primarily (been) pointing folks to the ES-C2M2 website at DOE because once you get there, you have access to everything else. And I've also noticed that the model has been looked at so often that if you simply do a Google search on ES-C2M2, it points you directly to that website.

Julia Allen: Great, great. Well, Jason, first of all, I would like to thank you so much for leading this incredibly valuable body of work and giving CERT the opportunity to actively work with you and participate in this effort. So, I thank you so much for your time and preparation today.

Jason Christopher: Thank you. Thank you very much for having me today. This was a great conversation.

Julia Allen: And Nader, thanks for being with us on the podcast series and leading the CERT charge to support Jason in this effort.

Nader Mehravari: You're quite welcome. And truly, I feel privileged to have been, have had the opportunity to be part of this effort following the footsteps of others from DOE, utilities, and CERT, who started this effort back in 2012.