Using the Cyber Resilience Review to Help Critical Infrastructures Better Manage Operational Disruptions
Transcript

Part 1: Purpose and Scope

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Program 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'm very pleased today to welcome Kevin Dillon with the U.S. Department of Homeland Security (DHS). Kevin is a Branch Chief for Stakeholder Risk Assessment and Mitigation.

I'd also like to welcome back my colleague, Matt Butkovic. Matt is CERT's Technical Portfolio Manager for Infrastructure Resilience. And I think you'll find today's topic pretty interesting if you're in the critical infrastructure space, as we will be discussing the DHS Cyber Resilience Review.

So, with no further ado, really pleased to have you on the podcast series, Kevin. Thanks so much.

Kevin Dillon: Oh, appreciate it. Thanks for having us.

Julia Allen: And Matt, great to have you back. Welcome.

Matt Butkovic: Good to be back.

Julia Allen: So, Kevin, why don't you help us set the stage a little bit for our listeners and tell them a little bit about the purpose of the Cyber Resilience Review (CRR). What is your objective in having stood this program up and conducting these reviews?

Kevin Dillon: Sure, Julia, thanks. So, it goes back to 2009. And really back then we were looking at ways to partner with critical infrastructure owners and operators, state, local entities -- really interested parties that were looking at ways to “improve their cybersecurity, both resilience and then protective activities.” We had longstanding partnership with the CERT program.

So, it was important for us to develop a way to help these owner/operators look at themselves and investigate things. And I think as most folks know, or maybe those listening to the podcast, obviously the vast, vast majority of critical infrastructure is in private sector hands.

So, again, this was really a way to look at those organizations and develop what we believe was a unique way, partnering with CERT and using the Resilience Management Model (RMM) as a background, to look at ways how organizations are prepared to handle a disruptive cyber event.

We're not putting a stake in the ground saying we have a methodology that says, “You are this secure or you have this kind of protective activities.” It's really how well can they handle a bad day.

Volunteer organizations come to us through all the sixteen critical infrastructure sectors. And, again, going back, we do, do a lot of work with state, local, and tribal, territorial governments. And we're trying to just basically understand their overall cybersecurity, how they manage critical services, the assets that are associated with that, really what's those mission critical functions that an organization is delivering.

And how do we focus those activities, and talk about the 10 key domains from the Cyber Resilience Review that really hope to mature an organization, move them to the right, whatever term we want to use to get someone doing a little bit more than they're doing today to help increase overall cyber resilience.

So, through using the Cyber Resilience Review, voluntary participants really can start to develop an understanding of how their operational resilience is in place, how they can manage those bad days with that cyber risk to those mission critical services that they're delivering, and really how repeatable and how well do they do those.

I always say people say they may be looking for a magic bullet or a way to say, “Am I secure?” And really, I think the importance of the CRR is, again, we're not saying that, but we're saying how well can you handle that bad day, how well can you handle that operational stress.

And so, we're looking, again, we talk about key management practices from personnel within an organization. Some examples we have there -- obviously many times we may be working with CIO office a CISO office, maybe it's the CSO. And we try to bring a sort of cross-functional personnel in place. That may be the IT security staff. It may be some folks from the business continuity staff. It may be the operational folks and sometimes either some physical or facility security personnel. So, it's a good mix overall of folks. But that's really the purpose in a nutshell.

Julia Allen: So, Kevin, do you feel that the CRR -- and I know we'll get in with you and Matt a little bit about the method description and how it works -- but in your experience, have you found that it works for organizations of all sizes? Or does it have a sweet spot of organizations of a particular size? Or does that really not matter?

Kevin Dillon: I think it's a great question. Maybe I'd be able to answer it in terms of maybe type of IT security staff size. So, we've had experience where we've gone to an owner/operator that -- give you an example -- two folks run everything. They've got the secondary, tertiary, and beyond duties, duties as assigned.

And at times, while it's obviously going to help them, they may struggle to answer the vastness of the ten domains and the ideas and the concepts that come across. They may not be at the maturity level where they can -- they have those things in place. But nevertheless, there's nothing punitive or negative about it. We're trying to help folks move to the right.

So, I would say the mid and up in size of staff is probably the best fit. I look at more staff size and how spread apart those -- which we'll get into -- the domains are in terms of is that a business line or a business function, or are lots of those duties, again, assigned to a small staff where they're really stretched thin?

Julia Allen: Got it. Got it, thank you. So, Matt, can you tell us a little bit about -- Kevin spoke a bit about when this all started. But talk a little bit about how the Cyber Resilience Review method was developed and get a little bit further into the topics, or we call them domains, that it covers. Can you say a little bit about that?

Kevin Dillon: Sure, Julia. So, as Kevin was explaining, there was a need to interact with the owners and operators of critical infrastructure in a way that gave DHS visibility into their ability to handle disruptive cyber events, but to elicit that information in a way that was lightweight, repeatable, portable. And it was agreed early on that this needed to be something that you accomplished in a single day. So, with that as a design constraint, we set out to build a lightweight cyber resilience diagnostic method.

So, that comes with some challenges. There are ten domains, as was mentioned earlier, in the CRR: asset management, configuration and change management, risk management, controls management, vulnerability management, incident management, service continuity management, external dependencies management, training awareness, and situational awareness. And the CRR addresses four asset types: people, information, technology, and facilities. And for most listeners that are familiar with the CERT Resilience Management Model, this will all sound very familiar.

The CERT-RMM was used as the foundation for the CRR. So, we selected practices, goals from the various process areas in the RMM, and articulated them as a set of questions and assessment method for the CRR.

There are a total of 269 questions in the CRR. And I think one of the unique distinguishing facets of the CRR is that our questions not only address the absence or the presence of a practice and its execution, but also we consider the maturity with which that practice is executed. So, there is two dimensions of capability being measured in the CRR.

With that said, one of the design principles was we must keep this simple and portable. Therefore, we have a very simple and digestible answer range for all those 269 questions. There are three possible answers: yes, incomplete, and no. And we felt that this simplified Likert scale was one of the keys to getting those consistent answers and consistent understanding through the various stakeholder groups that we visit.

Julia Allen: Great, and so as I listen to you name the ten domains -- many of which obviously are very familiar to me, Matt, as you and I have worked with CERT-RMM for some years now -- I hear the word management in these domain titles a lot.

And so, I think for our listeners' benefit, is it fair to say that what you take away from that is this is how these -- focuses on how these processes are managed, how the service is being managed to be resilient, how resilient the assets are from a management perspective as contrasted with going into detailed technical controls like NIST 800-53? Is that a reasonable description?

Matt Butkovic: Yeah, absolutely, Julia. Thank you, that's a very important point that we're really focused on operation resilience or operations management in the CRR. So, this is not a technical deep dive on a specific platform or technical safeguard. Rather it's an evaluation of the management processes that surround your cybersecurity program.

Julia Allen: Great. And also I'll mention, just put in a little plug for our listeners' benefit. There are many podcasts and other supporting materials on the CERT Resilience Management Model for listeners that aren't familiar with that work. So, I would refer you to those.

Part 2: Conduct and Results

Julia Allen: So, Kevin, let's get into how CRR actually happens, how it's conducted, a little bit about the results. If you're able to say maybe how you actually arrange with sites to participate. So, just give us a little feel about how the CRR rolls out.

Kevin Dillon: Yeah, absolutely. So, the CRR is a one day event, meaning we ask for the owner/operator to park aside, set aside, a business day. The DHS team and the CERT team come on site at the owner/operator's request. And it's a facilitated interview.

So, we sit around the conference room and we get the key cyber security personnel from the organization in the room. We bring a DHS federal staff, and then we also have a CERT staff with us. So, really that's important because as we're asking the litany of questions throughout the day, you really need those two people taking notes, asking follow on questions, really basically backing each other up so that at the end of the day, we can sit down together and go over notes and compare and contrast.

So, as Matt just alluded to, the 10 domains, you ask all the questions associated with that, really look for those yes, incomplete, and no answers. We want organizations to tell us more than yes and no though. It's a great conversation. And if someone's just continually saying yes or no, obviously we're going to ask, “Okay, how do you come about getting to a yes?” Again, not an audit, but we want to make that sure we're asking and hearing the right things from an organization.

So, we spend a great day with the folks in the room. And it obviously results in a report. That report is going to summarize strengths and weaknesses across each of the domains. And then we definitely provide options for consideration. That's our basically term for recommendation. But we had to soften that up a little and just say its options for consideration. And those contain guidance and activities that would help an organization improve. So, if they were showing lower maturity indicator levels in a certain area, we want to be able to offer them a path forward, steps to take to be able to make those improvements.

Again, the CRR, so it is no cost to the organization when DHS comes out. The only cost is the time involved from the personnel that are there. We strive to have those results and those options for consideration back to an organization no later than 30 calendar days after a visit. We're certainly usually a little bit faster than that. But if our resources, or we've been doing a lot of travel, then sometimes we might bump up against that thirty day mark.

So, we issue a draft report. And we want to have an outbrief with the organization when we do that, go over all the findings, go over next steps, maybe some highlight things that they could be working on first and foremost, and then give the organization an opportunity, obviously, to give us feedback if we mischaracterized something or we didn't use the right terminology that the owner/operator uses. We want to be able to make those adjustments for them.

And really, so when they see the report, a couple things to highlight would be the performance or the maturity indicator levels, and the by domain -- score is a bad word -- but results is shown in a series of heat maps and graphs. And then this also includes a comparison of the performance of that organization against all other prior CRR participants. Now, that's not in name. It's just in general total score, all aggregated together.

So, organizations asked us for that from the very beginning when we were going, so they can use their CRR results to look at how others are doing in these domains. And that's been a very valuable thing for folks to do. We've completed over 300 of these to date. And wide variety of organizations, sectors. We've done 12 of the 16 sectors.

And I guess one of the final notes I would point out here is that all CRR results are afforded protections under what's called the DHS Protected Critical Infrastructure Information program. It's a mouthful. But the acronym PCII -- it's very important that that gets out there, though, because those -- that result and that engagement that we have with the owner/operators is just that. It's an engagement between DHS, the owner/operator.

The end result, that report, is for the owner/operator use only. We don't share those results with anyone. We're trying to individually work with these owner/operators and do that. So, certainly, if someone were more interested in learning about the PCII program, a Google search, DHS Protected Critical Infrastructure Information would give you all the highlights. But, obviously, we'll have our contact information at the end to give you more on that.

Julia Allen: Great, great. And I'm really fascinated by this benchmarking idea because, obviously, in any kind of endeavor like this one, everybody wants to see how they compare with their peers. And so, when you actually share that kind of information, and obviously as you do more CRRs that kind of data gets better.

What's a typical reaction to a site when they see how they stand up, compare good, bad, or indifferent against the existing data that you have? Do you have any interesting anecdotes about that reaction?

Kevin Dillon: I would say what was surprising to me at the very beginning before we had 300 things to look at, or the universe of data that we have now, was how you could finish question 282 at the day, and at the end of that, the first question asked was, “How do I compare against either peers or the entire universe?”

So, obviously, we took that call to action and working with you all, the CERT folks, that's a really important piece to that. I think the results speak for themselves, meaning this is folks that are voluntarily meeting with us. They are looking for new and unique ways to manage the critical services that they run.

And I have yet to have a negative feedback, whether as you said, if their results may not be a gold star, or maybe they're above all the rest, it's always been taken as this is important for the owner/operators to be able to see that. Either one, pat on the back, or it's a way to communicate a path forward and maybe some goals to strive for if they need to use it that way.

So, yet to experience anything other than that's something that's been from day one, critically important for us to be able to do based on the feedback we receive.

Matt Butkovic: I would add that seldom is site surprised by the results. I find that we're usually confirming in the structured conversation things that an organization already knows about themselves. And I think one of the chief benefits of the CRR is convening that team of people that can have that conversation about subjects that oftentimes organizations don't make the time to have.

So, as Kevin said, positive reactions universally. And I don't think it really needs to surprise anyone. I think we're largely confirming things they knew, but providing them with the structure to understand if they're to make improvements, where they might want to focus their attention.

Julia Allen: A follow up question for either of you -- so as I think about going out on these and giving folks comparative information on where they stand with respect to others and also providing things, improvement activities for them to consider, have you had an opportunity where you find at one site, a particularly effective set of practices or ways of implementing the domain that you've been able to share anonymously with another site who's looking to improve in that area? Do those kind of conversations take place?

Kevin Dillon: They do, and I think it's incumbent upon us to ask. So, we've had these really great examples where it's really encouraging to see all these great things happen and do just as you said.

We ask them for, obviously, a sanitized version, or maybe an outline of a plan that seems to be really successful for an organization, and then to be able to include that as a follow on to reports with other like organizations. So, if they were in the same sector or same critical business area where we evaluate it against the same type of service, those are great follow-ons.

Part 3: Analysis of CRR Data and Future Plans

Julia Allen: Great. Great. So, Matt, let's talk about the data a little bit. There are these 10 domains. There are 269 questions. There's yes, incomplete, no. I know your team, from my observation, has done a lot of great work on automating and making that kind of data easy to analyze. So, can you say a little bit about the kinds of data that you're collecting and how the data's being used today?

Matt Butkovic: Sure, certainly Julia, I think that this is one of the highlights of the program. The CRR collects data in a way that is in strict adherence with PCII. That means the data is not attributable, we only use aggregated, non-attributable data in any analysis that were performed.

The CRR is structured around the concept of a critical service. So, we ask these 269 questions from 10 domains in relation to a specific activity the organization sees as key. For instance, in the water sector, it would be the purification and distribution of potable water, an example of critical service. So, think of that as a piece of demographic information that accompanies the data we collect.

We then take this data and the first use is for the site itself. We create a report that contains detailed information about each of the questions, the answers provided, and then, as we discussed earlier, heat maps, graphs, and then options for consideration.

The secondary use of the data is to look for patterns and trends in the larger dataset. And we've leveraged techniques and tools with some partners on campus here at Carnegie Mellon to ensure that we're doing this in a rigorous and scientifically sound way. And I think this is really one of the emerging highlights of the program is that we're now seeing patterns and drawing conclusions or finding insights regarding the performance in the cyber resilience of critical infrastructure organizations.

I think in many ways this is unique. And Kevin's program is uniquely positioned due to the CERT-RMM and the collection methods of CRR to really examine the operational resilience of the organizations that participate in the CRR.

As we spoke about a little earlier, there's this comparison view in the CRR report. And you know, to state the obvious, collecting the data then allows us to do comparisons and feed that back to the participants.

Julia Allen: Is there a -- not to put both of you on the spot -- but Matt, are there any plans to, even at a summary level, to make some of that comparative or trend or pattern data publicly available?

Matt Butkovic: Sure, so I am very proud of the reporting that we've done and the insights that we've collected. And I think, not to put Kevin on the spot, but I think it might be in the realm of possibility that we'll see some public versions of that summary data in the future.

Kevin Dillon: Yeah, Julia, absolutely. So, we want to be able to do that and that's the -- not to get ahead of ourselves, but a big evolution of the main goals of the CRR is really to be able to take data and do important things with it, and be able to make, put out options for consideration in kind of general terms, or path forward and implementation guidance for organizations that are looking for ways to improve their operational resilience. So, absolutely, that's a key goal is we build it, the right data, and we get enough information to be able to do that, that is the main goal.

Julia Allen: Great, so Kevin, you're into my -- nice lead into my next question for you, which is as you started to discuss a little bit about the near-term and perhaps the longer term future plans for the method and how you might see using it going forward?

Kevin Dillon: Yeah, absolutely. So, we always want to evolve. We always want to be doing better, learning, taking feedback, continual improvement, if you will, really just to make the one experience as best as it can be for the owner/operators that are participating in this. They're volunteering their time. They're working with a government agency to do this. So, we want to make that very valuable to them.

A couple things I think I'd like to highlight are pretty exciting. We're in the early stages and have done some preliminary what we call Cyber Resilience Workshops. So, back in some of the previous discussions, you did ask about is there a right size organization for this? And we don't have that defined, but I think the example of a Cyber Resilience Workshop here may fit, in that if you had a number of organizations that, in discussing the CRR, may not be ready. They may be in a state of flux in terms of maybe going through a technology transition, or they've had a large turnover in personnel or something of this nature.

But they're still interested in the concepts. We've been able to take again the CRR domains, the concepts of cyber resilience, working with CERT and working with our DHS staff, and build that into a workshop.

So, you could get twenty or thirty entities, or twenty or thirty folks from an organization -- it really just kind of depends, and be able to do a workshop on these concepts. So, they wouldn't necessarily be going through a CRR but get a lot of that great information that we have.

As we just mentioned before, as the dataset continues to grow, that's the big deal. That's how we get to be able to say things, be able to offer areas for improvement, maybe not even areas

for improvement, just great practices that we've seen, again the other example that you gave, and be able to share that with our stakeholders and partners.

And then another piece that I'm excited about is we already ask about external dependencies and how those are managed. But in the context of supply chain risk management, and the tie to those external dependencies on either ICT service providers or folks that you're doing business with and are critically important to the success of your business, we want to really be able to enhance and dig in deeper on that external dependencies piece.

So, that is -- we're doing that now. I would think if we're talking six months to nine months down the line, we'll be a little bit further along. And I'm pretty excited about all of that.

Julia Allen: Great. Great. And Kevin or Matt, do I understand correctly that we're actually in the process of developing some implementation guidance specific to each domain? Do I have that right?

Matt Butkovic: Yeah, that's correct, Julia. So, we, as something to augment the CRR experience and to provide a lasting leave behind artifact, we're building a series of guides, one for each of the ten domains. So, that once the site has a CRR and are presented with options for consideration, they're given a more robust road map that says, “Here are the things we'd recommend you do to close this gap.” It's another exciting piece of work, and I think another example of how the program is growing and to not only just an assessment method, but a data analysis program and a program that's generating artifacts for the larger critical infrastructure community.

Julia Allen: Great. Great. So, Kevin, obviously everybody that's listening to this podcast, and everybody that they're going to refer to to listen to this podcast, are all going to want to sign up to do a CRR with you. So, could you say something about if someone does want to pursue that, what next steps they should take?

Kevin Dillon: Sure. The best way is to email the program. And that is CSE (for Cyber Security Evaluations) @hq.dhs.gov. And the email is direct. The program folks will get it. And we, there's a person on the other end. So, we contact them back directly and would obviously set up conference calls and go through the primers and all the background information to get them set up and do that.

Julia Allen: Great. And obviously, we've just touched the surface on many aspects of the review today. So, do you have some pointers to additional information for our listeners?

Kevin Dillon: The best way for information about the CRR is just to email us direct. For general information about DHS's cyber initiatives, dhs.gov of course. And obviously you have the CERT-RMM references. I'm sure Matt will key those up.

Julia Allen: Right, so Matt I know on the CERT side, as Kevin indicated, there are a couple things that we have. So, where would you point folks for additional information?

Matt Butkovic: Sure, there's a wealth of information not only about the CERT-RMM, but also about maturity models and various facets of managing information security at the CERT website. I'd highlight for the listeners a prior podcast from June of 2013 entitled "Managing Disruptive Events." This explains how all the CERT-RMM can be used to evaluate and manage your cybersecurity posture.

For those listeners interested in the CERT-RMM, www.cert.org, the resilience page, you'll find information about the model itself and then the various activities and artifacts we have of support use of the CERT-RMM.

Julia Allen: Well, Kevin this has been great. We covered so many interesting topics and, as I said, pretty much just got the tip of the iceberg. But I so much appreciate your time, and your leadership, and your application of taking the CERT-RMM and applying it to a very important national problem. So, thank you so much for your time today.

Kevin Dillon: Oh, you're welcome. Thank you.

Julia Allen: And Matt, always great to have you on the podcast series. Your team is doing fantastic work. And I appreciate your time and preparation today as well.

Matt Butkovic: Oh, thank you for the opportunity.