Managing Disruptive Events: CERT-RMM Experience Reports

Part 1: U.S. Department of Homeland Security Cyber Resilience Review

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 our podcast website.

My name is Julia Allen. I am a principal researcher at CERT working on operational resilience and measurement. I'm pleased to welcome back my colleague, Nader Mehravari. Nader is a member of CERT's Cyber Resilience and Measurement Initiative. And today -- you've heard Nader and I talk before -- but today he and I will be capturing the third in his three-part series on principles and practice of operational resilience.

For our listeners that have been tuning into that series, I think you'll really appreciate that what we're going to talk about today are some case studies and some success stories, specifically experiences of four organizations who have successfully applied the CERT Resilience Management Model across quite a wide range and a diverse type of operational resilience objectives, which I'm sure you'll appreciate hearing about from Nader.

And I also wanted to mention that we refer to the model as CERT-RMM, or just RMM. And if you aren't familiar with it, we have posted several podcasts and webinars for background information so I would refer you to those.

So, Nader, I really appreciate having you back on the podcast series, so welcome.

Nader Mehravari: Hi, Julia. I'm delighted to be back.

Julia Allen: So to help bring our listeners along, it's be a while since we've spoken, are there any summary key points from your first and second podcasts that you would like to recap before we get into today's discussion?

Nader Mehravari: So we started this series in the first podcast by setting the stage by talking about how organizations are under operational stress on a minute-by-minute basis. And we illustrated that through referring to some incidents that we all have seen over the last 12 months in the news, and maybe even been affected by -- and how these disruptive events, at times, were very surprising to folks who were affected and also those who were planning to be prepared for it.

And we pointed to some shortcomings given how complex our business processes are today and how our business is dependent on resources all across the world. And then we came back on a second podcast, and we discussed the question of, “Are there better ways to deal with disruptive events?” And that led us to discussion and deduction of concepts of resilience and operational resilience.

That's when we start talking about the CERT Resilience Management Model, which is an overarching framework for organizations to use to assess, improve, and manage their operational resilience. And our plans today in this third and final segment is to share how several organizations have successfully done that using CERT-RMM.

Julia Allen: Great, so I think that anybody that's new to this model, and to the body of knowledge that it represents, will benefit from learning about some examples of how organizations have actually used it.

So let's start with the U.S. Department of Homeland Security. You and I both know that they're using concepts from the model to conduct what they call Cyber Resilience Reviews to help assess the security posture of critical infrastructure organizations. So can you describe that work a little bit and how you've seen the model applied in that context?

Nader Mehravari: So, what the Department of Homeland Security, or DHS, is doing is actually very important. Because after the 9/11 events, one of the facts that became very visible to all of us in this country is that 85% of our nation's critical infrastructure is owned and operated not by government but by private sector. And therefore DHS, as part of their mission, was very much interested in getting a pulse on how prepared operators and owners of critical infrastructure are.

So the primary purpose of this program that DHS has put in place, Cyber Resilience Review (CRR), is to assess the cyber security risks to our country's critical infrastructure and associated key resources that makes those critical infrastructures enabled.

The program that they put in place is something that CERT was involved in developing. It is based on CERT-RMM framework. We can say it's a derivative of RMM. And it basically enabled DHS to perform better, efficient review of overall practice integration and health of an organization's cybersecurity program.

Julia Allen: I'm kind of curious because I know they took actually only a subset of the model. They had specific domains or specific topics that was of greatest interest. So can you say a little bit about the scope of the Cyber Resilience Review as compared to the entire Resilience Management Model?

Nader Mehravari: Right, so one thing that I mentioned in our second podcast, that the RMM model is very comprehensive. And one of the first things that entities and organizations who want to use it should be doing is to determine which part of the model makes sense to use for their particular activity. So that's exactly what DHS did.

The first thing to determine was determining, “Okay, who is the target organization that they are going to apply the model to, or a substantive model to?” That organizational scoping was important, and they wanted to apply to critical infrastructure and key resources providers and also some of the state, local, or tribal government agencies.

The next question they asked was, "Okay, if I'm interested in asking questions about cybersecurity preparedness and cybersecurity posture of these organizations, which part of the model from the process areas should I consider?" So they selected 10 and as we mentioned before the RMM model has 26 areas.

The 10 that they picked are very much related to the things that an organization should be doing in order to improve their cybersecurity. It starts anywhere from dealing with access management and control management, vulnerability and incident management, all the way to some more fundamental concepts such as risk management and learning about situational awareness. So there were approximately 10 domains that they had selected.

Julia Allen: And how is a Cyber Resilience Review actually conducted? What are some of the events that take place to make one happen?

Nader Mehravari: Yes, very good question. So, as we said, 85 percent of the critical infrastructure is owned and operated by private sector. That should give us a good indication that there are many such organizations. And therefore DHS was looking for a methodology that is very efficient from a perspective of the resources it takes to implement it and also how long does it take to do one of these assessments.

So the approach that is used to do each one of these reviews -- it's very compact, it's very efficient. It starts by selecting a particular location. That location is provided with some pre-assessment questionnaire before the site is visited. The actual site visit is only one day long. A very small number of individuals visit the facility and they perform what we call a facilitated interview and data collection exercise.

And at the end of that day, a report is generated that does two things. It provides what strengths or weaknesses was observed and also it makes some recommendations for improvement. So it's very efficient, it can be done very quickly, and that was one of the major requirements for DHS for this program.

Julia Allen: Great, great. Before I move onto our second example, was there anything else you wanted to say about this activity or this case?

Nader Mehravari: No, this activity started to be designed three or four years ago and it's in steady state. I believe it's in the third year, and DHS is continuing performing these kinds of reviews across the country.

Part 2: U.S. Department of Energy Electricity Subsector Cyber Capability Maturity Model

Julia Allen: Excellent. So let's move on. I think the second one is a rather novel application of the model. So in 2012, I know the U.S. Department of Energy approached us, along with quite a few other organizations, as part of their leadership of the development of something that came to be called the Electricity Subsector Cyber Capability Maturity Model. It's a bit of a mouthful. We refer to it as ES-C2M2.

And I know from our participation in that work it was derived in part from the CERT Resilience Management Model. So can you say a little bit about ES-C2M2 for the electricity subsector and how it's being used today?

Nader Mehravari: Yes. In fact, we think this particular activity shows one of the most powerful aspects of the RMM model in a sense of how well it can be customized and adapted to very specific needs.

So early in 2012, as you mentioned, due to some sponsorship from White House, Department of Energy started asking the question, “Is there an efficient and economic way for them to assess the strength of the cybersecurity capabilities of owners and operators of various components of the United States electrical grid?” And these components include generators of electricity, distributors of electricity, those who control the grid itself, etc.

So their objective was to assess the strength of the cybersecurity capability of these elements. They wanted to enable themselves to have a consistent evaluation, a benchmarking of cybersecurity capabilities of those who are involved in making the national grid possible. And

use that consistent information of benchmarking, share it, and use any best practices they observe with the community. So that was their objective.

Julia Allen: And I know it was a very aggressive development schedule. Both the White House and DOE wanted to get something out for pilot use very quickly. And can you say a little bit about some of that development and early piloting experience?

Nader Mehravari: Right, so the model was developed very quickly within the span of three to four months using CERT-RMM and a few other bodies of knowledge. Within three months, a framework was developed to enable the Department of Energy to do this. Immediately it was put into practice by running several pilots, close to 20 of them, in that middle part of 2012.

Those 19 or 20 pilots demonstrated that, yes, the model -- that this derivative actually does what DOE was looking for. And enough data was collected in these 19 or 20 trials to make the model even more flexible and improvement based on that initial development.

Now the framework is being used on a regular basis by DOE to do a similar approach with like what DHS did for CRR. Again, it's a very efficient methodology. It's a one-day visit by a couple of subject matter experts, and those facilities are provided with feedback as to what strengths or shortcomings were observed and some recommendations for potential improvements.

Julia Allen: I don't recall but maybe you know, Nader. Is there also an ability to self-assess against this model or is it still an expert led team as far as you know?

Nader Mehravari: Right, so one very useful thing that the Department of Energy has done since the development of this framework; they have made it publically available. Anyone can go to the Department of Energy's website, download a full copy of the ES-C2M2 model, which explains the details, explains the type of questions that should be asked in an assessment, and there are self-assessment spreadsheets and tools that DOE makes available.

So, yes, self-assessment is something that some organizations are doing on their own using this model. In fact, that's one of the reasons that this particular derivative of RMM has become very widely publicized in the community because people are able to do self-assessment.

Julia Allen: And do you know, are organizations that use the model, either through the expert-led or the self-assessment, are they required to report their results? Is it voluntary? And as a follow up to that, is DOE using that feedback to improve the model?

Nader Mehravari: The organizations who use the model to do self-assessment, that's something they do voluntarily, and they're not required to report their findings to DOE. The ones that DOE performs using a subject matter expert in a facilitated way -- some of that information is available within DOE with the required guidance to protect that information, and that information could be used if the model needs to be improved, or expanded, or enhanced.

Julia Allen: Okay, great. So before we move on, anything else you'd like to say about ES-C2M2, Nader?

Nader Mehravari: The only other thing I would mention is, again, this exercise of development of ES-C2M2 has demonstrated to others in the community how a very extensive fundamental framework like RMM can be used to develop derivatives that are very efficiently and effectively can be applied to narrow domains.

In fact, it has been so publicized from a perspective that, hey, this is something that maybe other critical infrastructure sectors may consider -- that based on the recent Executive Orders for NIST, National Institute of Science (Standards) and Technology, to develop some global cybersecurity framework. NIST is considering experiences that people have gained by using ES-C2M2 as they develop their cybersecurity framework.

Part 3: U.S. Postal Inspection Service - Protecting the Mail

Julia Allen: Excellent, excellent. Well, let's turn our attention to one that you and I have been actively engaged together in and that is our work with the U.S. Postal Inspection Service. We have the good fortune to have a visionary, Greg Crabb, who we've captured a podcast with about their uses of the model.

But I would be remiss if we didn't have some conversation about their various applications because they've taken us in directions I certainly never intended. So can you say a little bit about their use of the model and also the tailored appraisal methods we've helped them develop?

Nader Mehravari: Right, so U.S. Postal Inspection Service, which is a law enforcement arm of the United States Postal Service which, by the way, they are the oldest federal law enforcement agency in this country. Their mission is to support and protect what the United States Postal Service does -- their mission, their employees -- and to support the U.S. Postal Service to make sure the mail that is transported in this country is safe.

So, with that mission in mind, they continuously do activities, which can be considered operational risk management -- making sure that our mail is safe. The things they do to make that happen is at the highest level their operational risk management. And therefore it was very natural for them to consider using a framework like RMM, which fundamentally deals with operational risk management. And they have done some very innovative things with it.

One of the most innovative applications of RMM, or the concepts within RMM, that the Postal Inspection Service has done has to do with actual physical security -- using some standards from the international organization that oversees movement of mail across the world, UPU (Universal Postal Union).

Using standards from UPU, we were able to develop a risk assessment methodology, a risk assessment instrument, for them to allow postal inspectors to assess physical security and physical safety of international mail centers at other countries. That's important because that is the origination point of international mail that comes to our country. And, therefore, if you want to make sure that mail is safe, we like to have some idea of how well physical security is managed in those facilities.

So they, with our help, developed a physical security risk management, assessment tool that is based on RMM, and the concepts that RMM is based on. And that has been very well received not only by U.S. Postal Service personnel but also the international organization I referred to, UPU, has now recommended the same methodology to be used by other countries to assess physical security of international mail centers.

Julia Allen: Great, great. What about some of the other applications that are more relevant domestically?

Nader Mehravari: So one point that I made about the RMM framework in our second podcast was that RMM looks at resilience management starting from the assets. It considers certain classes of assets that organizations have and asks the question, “What is the best way to protect and sustain these assets?” -- because those assets are the ones that are critical to ensuring an organization's mission is enabled.

Now, the framework itself talks about four types of assets that are very strong resilience consequences: information assets, technology assets, people assets, and facility assets. Now, the model is flexible enough that if an organization's mission requires them to deal with different types of assets, that the model can easily be expanded to include that specific type of asset. So that's what U.S. Postal Inspection Service has done. With our help, they have developed additional process areas in the model that deals with mail pieces.

The United States Postal Service -- its primary mission is to collect and deliver mail pieces, and therefore mail pieces is a critical asset to them. So they have expanded the model by adding a new asset to the model and therefore, they can do more focused assessments and risk management dealing with mail pieces. So that's also been a very interesting application of RMM that demonstrates its flexibility and its capability to be expanded to cover different types of assets.

Julia Allen: Right. And I know from our experience working together we actually are in the process of helping them evaluate Express Mail against these new process areas including one for revenue assurance. So did you want to say a little bit about our Express Mail work?

Nader Mehravari: Right, so express mail is one of the more important services that USPS provides, particularly for the business sector. And it is one of those services that the value of each Express Mail package is a high value compared to the standard First Class Mail pieces that you and I use on a regular basis. And therefore, it's important to assess and have a good idea of the risks associated to the revenue that, that particular mail stream generates for USPS.

So, in that sense, risk to revenue is considered an operational risk for USPS when we look at the Express Mail stream in the postal system. And therefore, U.S. Postal Inspection Service has used some of these additional process areas that we have developed for them, in particular mail revenue assurance process area, to assess revenue risk associated to the Express Mail stream.

Julia Allen: Great. Well, in the interest of time, Nader, I'd like to move onto our last case, but I do, as I mentioned earlier, I do refer our listeners to a podcast that we captured with Postal Inspector in Charge, Greg Crabb, if they're interested in learning a little bit more about this particular application.

Part 4: Lockheed Martin Corporate Business Resiliency Strategic Initiative

Julia Allen: So let's talk about your former organization, Lockheed Martin Corporation. That's how we came to know one another. You were actually one of the thought leaders within Lockheed Martin bringing in the use of the CERT Resilience Management Model as part of your efforts.

So can you say a little bit about the Corporate Business Resiliency Strategic Initiative -- both how you started to use it when you were there and how it's being used today?

Nader Mehravari: So Lockheed Martin Corporation, a large commercial entity in this country with operations in countries around the world, is an example of a commercial entity who has been using RMM for several years.

The initial interest at Lockheed was to identify an overarching framework that would allow them to initially measure or assess resiliency posture of the organization; use that as a mechanism to determine whether the current posture is sufficient for their business needs; whether they'd like to set a goal to improve their current posture, again, based on business needs; and then, use the model again to continuously measure and assess themselves as improvement mechanisms are executed; and also determine when they've reached a goal; and on a regular basis, again, measure and assess themselves to make sure that once they achieve their goal they stay there.

So the initial purpose of using the model was to provide a, let's say, a common and consistent ruler to assess and measure resiliency posture, either across the corporation or within different segments of the corporation.

The model has since been used for other purposes at Lockheed Martin in addition to applications for measurement and assessment. It has been used to guide how best to integrate some of the existing risk management activities such as disaster recovery, business continuity, and crisis management. That's one of the fundamental capabilities within the model that guides organizations to do that.

The model also have been used for providing a common vocabulary across the organization. Even if entities are not using the process areas, it's just used as a mechanism to provide a common language.

Julia Allen: One of the things I found fascinating about the Lockheed Martin work -- it helped make clear to me that the model, RMM, can be used to help assess intent. So you take a look at some area of interest and you evaluate it against part of the model to see if in the future, if you are going to undertake an improvement initiative, if you've got your intent properly described. And then, as you said earlier, you can actually then assess how that plays out.

So you can assess or appraise for intent, and you can also assess or appraise for actual implementation. What am I doing today? And does my current state have gaps in it that I need to address? So I found that whole idea of assessing for intent against the Lockheed Martin policies, or what they call command media, I thought that was a very innovative approach.

Nader Mehravari: Right, I think that's one of the strengths of the model, in a sense, that many organizations across the world have in place policies and procedures that dictates or drives their risk management activities. If those policies and procedures are not well structured, then clearly the activities that are implemented based on them may not be as efficient either.

Therefore, assessing intent by assessing those policies or command media as you mentioned -- it's an easy thing to do using the model, and they have powerful consequences because then you can decide, “Oh, there are major shortcomings in our policies and procedures. Or, there are strengths in one policy that we should replicate in other policies.”

Julia Allen: Great, great. Well, Nader, I think we need to wrap this up, and I wouldn't be doing justice to our listeners if I didn't give you a chance to point them to some additional resources that will elaborate some of the things we've talked about and point them to content that may be

helpful for them if they want to apply the model. So could you give us a few of your favorite resources for more information?

Nader Mehravari: So for those listeners who have not heard the first two segments of this podcast series, I recommend to listen to that, to the first and the second podcast where this is the third one. Much of the subjects that we've talked about during these three podcasts are based on a tutorial that I delivered last year at the IEEE Conference on Technologies for Homeland Security. So the slide material from that tutorial is another good starting point for folks to get familiar themselves with the concepts of operational resilience and CERT-RMM.

And the most recent item that listeners might be interested in, on April 30th of this year, as part of a day-long series of webinars, webinars at CERT, which was titled, “Discussions with CERT Experts,” I had an opportunity to have a segment to deal with how organizations can go about assuring their mission using concepts of operational resilience. So that is another resource that our listeners might be interested in -- in addition to all the resources that are available at the CERT's RMM and Resilience websites.

Julia Allen: Well, Nader, this has been terrific. I'm sad that our podcast series is coming to a close, but I know we'll have ample opportunities to talk on additional subjects in the future. So thank you so very much for you time and your preparation today.

Nader Mehravari: You're quite welcome. It's been a pleasure for me to participate in this series.