How Resilient Is My Organization?
Transcript

Part 1: Resilience: The Convergence of Security, Business Continuity, and IT Operations

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, 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 senior researcher at CERT, working on operational resilience and software assurance.

Today I'm pleased to welcome back two of my CERT colleagues to our podcast series. First you'll be hearing from Rich Caralli, who's the technical manager for CERT's Resilience Enterprise Management Team, and Dave White, who's our team lead for Resilience Management and the Resilience Management Model.

Today Rich, Dave and I will be providing an update on CERT's work on the Resilience Management Model, version 1. It's been a while since we've talked about it, and it is described in a publicly available report from the SEI. Also version 1.1 of the model is described in our new book, The CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience.

Before I introduce Rich and Dave, I just wanted to mention in interests of full disclosure I am a member of this team but today obviously I'm serving as moderator. So welcome back, Rich.

Rich Caralli: Thanks Julia. Good to be here.

Julia Allen: Okay, Dave, and glad to have you with us today.

Dave White: Thanks Julia, always a pleasure.

Julia Allen: Okay so Rich, as our fearless leader, it's been a while, as I said, since we last discussed all the work we've been doing in operational resilience at CERT. So by way of a refresh, can you say a little bit about why this is increasingly becoming a high priority topic for the program?

Rich Caralli: Sure. So I think that we learned through many years of research into security and security management that the ultimate goal of what we do as security professionals is really resilience. It's the end-game. We've seen that attitude change in the last 10 years where a lot of the work that we did in security was for security sake, to stop something, to prevent something, when in actuality what we were trying to do is to enable something bigger, like the mission of the organization.

And so we now view security at CERT, and the activities associated with security and the discipline, as a means to resilience. Part of that is because the complexity of the operating environment that we work in means that we can no longer be lured into thinking that we can prevent all threats and vulnerabilities from becoming risks. So we must take a multidisciplinary approach that also limits impact. We have to look at it, in fact, from both a protection and a sustainability standpoint.

So at the end of the day, a threat or vulnerability only really matters if it can disrupt something important to the organization or important to us. So when we get to the concept of resilience, as opposed to just security, it broadens the organization's target, and it helps to focus all of these individual efforts that every organization performs in security and continuity and improving operations.

So I think that the 'resilience' term actually characterizes what CERT has been about all along, which is giving organizations the ability to control their destiny and to carry out their mission in the face of a very ever changing risk environment.

Julia Allen: Excellent. Well thank you for that. So to get into the model a little bit, for our listeners who are not familiar with the work we've been doing on the Resilience Management Model (RMM), can you bring it down? Briefly describe its purpose, perhaps some of the disciplines it covers, and who we're targeting as the intended audience?

Rich Caralli: Sure. Well I'll just say first off that talking briefly about CERT-RMM is often difficult. Because it does sort of have a lot of hooks in it for different uses, depending on your view of the world.

But I can tell you that after five years of work in developing the concepts and building the model of CERT-RMM, the purpose of the model has certainly evolved. When we started working on this project in 2004, we simply had the objective to codify a maturity model that would characterize the important activities an organization needed to perform that would ensure it had some chance of controlling its destiny in stressful times.

I think that, over time, particularly the last six years, the purpose of the model has evolved toward many other uses that can be seen depending on your vantage point. Ultimately through development and application we saw a larger purpose: the ability to transform a community or an industry to a resilience view.

And thus the purpose of the model is really to provide a basis for an organization's transformational journey, from one that approaches stress and disruption as an ad hoc get-lucky activity to one that can really put the organization in control of its destiny.

I think we realized throughout our journey that many organizations unjustly had strong confidence in their cyber security or their cyber resilience posture, simply because they happened to get lucky in handling some stressful times, or that things didn't occur that they knew about.

However, the wrong time to find out that you can't handle a stressful time is when you're faced with it. So the model gives people a way to determine their capability for handling stress with justifiable confidence that they will not only survive challenges but also thrive in them.

So to the resilience end, the model really includes three disciplines what we call 'convergence' in the model. It tackles the security activities, the business continuity and disaster recovery activities, and it has some considerations for IT operations management. Thus if you're involved in improving any of these disciplines, the model should be useful for you.

The audience for CERT-RMM is really anyone interested in improving the mission assurance of high-value services through improving operational resilience processes. So that's a lot of words. But what it basically means is the model is useful for improving the way we do security and continuity and IT operations activities, with the view or the focus on improving the organization's ability to reach its mission, repeatedly and consistently over time.

So simply stated, CERT-RMM can help improve an organization's capability to meet its commitments and objectives with consistency, with predictability, in the face of changing risk environments and potential disruptions.

I also wanted to say that if you're a large enterprise or organizational unit, or you're a small mom and pop shop, CERT-RMM is certainly scalable up and down those different sizes of organizations. And when we built CERT-RMM, we really did not set out to displace the use of codes of practice such as ISO 27000 or COBIT or ITIL. Those codes of practice that are at the tactical level are all cross walked back into CERT-RMM. So it provides an overlay over that, to make those processes and those practices more efficient.

And certainly if you're a member of an established process improvement community, particularly one that's centered on CMMI models, CERT-RMM allows you to extend your process improvement knowledge from the early lifecycle phases of software and systems development into the operations phase of the asset lifecycle. Thus, process improvement doesn't need to end when an asset's put into production. It can continue until the asset is retired.

Julia Allen: Great, great. Thanks very much. I know there's a lot covered. A lot of years of work have been going on. So I know it's hard to bring it down into a nutshell but I appreciate that description.

Part 2: Structure and Use

Julia Allen: So Dave, let's give you some airtime here. Can you say a little bit about how the model is structured, maybe to give a visual or a little more tangible description about what the model is, how it's structured, how it breaks down into its component parts?

Dave White: Sure. So the model, at the highest level, consists of 26 process areas. For people who aren't familiar with how a model like this is structured, you can just think of those as the 26 chapters of the book that the model is. Those are the highest level decomposition, if you will, of the model is 26 process areas.

We've organized those 26 process areas into four categories, to highlight the similarity of different groups of process areas. The first category is engineering process areas there are six process areas in that category. And those are the process areas that help an organization identify the assets on which its continued operation depend, and then to establish and implement strategies to protect and sustain those assets so that the organization can stay in operation.

So that's the Engineering category. The second category is Enterprise Management, which includes seven process areas. And those process areas address high-level enterprise-focused activities that are really foundational to managing resilience activities across the enterprise. And even though they're focused at a high level in the organization, in various organizations we have found that they're implemented at various levels.

But they are high-level activities from an organizational perspective generally. The Operations Management category, the third category, contains nine process areas. So that's the largest category. And those process areas represent the day-to-day, ongoing, day in/day out activities that are necessary to be successful in managing operational resilience.

And the fourth category is Process Management, and there are four process areas there that help an organization implement, measure, monitor, and improve processes, that support resilience activities over time.

So those are the four categories, 26 process areas. Each process area is composed from a set of specific goals, which are supported by specific practices. And if you look at the entire model by the numbers, we have the four categories, 26 process areas, 94 specific goals, 251 specific practices; and then there are three generic goals and 13 generic practices that are applied to each process area in the model.

For those listeners who may be familiar with the CMMI product suite, the architecture of the RMM is very similar to the architecture of CMMI though I think we made some improvements on that. But it has the same basic structure. The RMM is a continuous representation model, which means that an organization gets to choose which process areas it wants to use, at which time.

So there is no prescriptive path through the model. There's only a path that an organization chooses through the model. So an organization can use as much of the model or as little of the model as makes sense, given the objectives they have. What have I missed Julia? Anything else I should add?

Rich Caralli: Well actually Dave, I'd like to add something, if possible. One of the things I think that's occurred to this team as it's grown larger is that the community has caught up to these concepts that we brought to light back in 2004 that the focus should be on resilience, and security should be a means to that, and that you could use a process model, and even maybe a maturity model, to really improve security and business continuity.

One of the things we're concerned about frankly at this point though is that a lot of maturity models are hitting the market. In fact, there's almost maturity model overload in this space now. And one of the differentiators of CERT-RMM from many of those models is that the capability levels in CERT-RMM the levels which give you a sense of how well a process has been institutionalized (meaning you'll retain it under times of stress, which is what this is all about) those have an empirical basis to them in our model. So those levels come from years and years of research and application that was done in the CMMI world. They're not arbitrary. And what we're seeing in a lot of maturity models that are being put out there is that the levels that are being used are arbitrary. They're not supported by any foundational concepts.

So when somebody tells you they're capability level 3 in CERT-RMM, what they're telling you is that they're being measured against a set of criteria that indicate that a process is being performed at a defined level, and that has meaning and foundation behind it. So we think that's really the big differentiator with CERT-RMM is that we didn't have to reinvent that maturity model undercarriage. We really used the best of CMMI to apply that to the subject of resilience.

Julia Allen: Dave, is there anything else you wanted to say about the model structure, or have we covered it?

Dave White: Well there is one more thing. So the model defines four capability levels: capability level 0 through capability level 3. For people who may be familiar with CMMI, this is a little bit different because CMMI defines six capability levels. We're only defining four capability levels for RMM at this point in time.

Julia Allen: And I know we've reserved judgment going forward, as more folks use the model, where we might actually allow for increasing capability if we observe that in practice, correct?

Dave White: Correct, correct. And that's a good point. Because our primary reason for limiting it to capability levels 0 through 3 is that that's all we've observed. We've worked with some really good organizations who collaborated with us in the development of the model. We haven't seen any of those behaviors that suggest that organizations in this space have institutionalized these activities at more than a defined level which is where the activities really become performed consistently across the organization. We haven't seen anyone go further than that yet. And when we do we'll add a level to the model, or two.

Julia Allen: Well let's talk about the model in application. I know we're early in actually putting the model into practice, working with organizations to use it to improve their practices. But I know you've been spending a lot of time in the field, Dave.

So could you talk a little bit about some of our current and early customer experiences and results; how organizations are starting to use the model; and maybe a little bit about at least what you're seeing in terms of early benefits?

Dave White: Sure. So it's a great pleasure to me that I get to spend a lot of time in the field working with organizations who are beginning to use the model. And a lot of organizations are using the model at this point in time for benchmarking and gap analysis activities, to evaluate what they have going on, as a precursor to or part of improvement activities to enhance their resilience posture and activities over time.

We're working specifically with a number of organizations who are taking different viewpoints on the model. So I've worked with an organization that is using the model to improve its information security activities and some compliance responsibilities around those information security activities and operations. I'm working with another organization that is using the model to improve its IT operations activities.

And I'm working with a third organization that is using the model to improve its business continuity and disaster recovery operations. That organization happens to be quite large, and those activities are interesting because they're focused at the policy level. So they're really focusing improvements, or making improvements, in the policy and guidelines that affect how these activities are done across the entire enterprise. It's a very interesting way to use the model and an interesting place to focus the model in an organization. So that's an exciting project.

We also have organizations that are using the model to evaluate critical infrastructure protection activities. We have some organizations that are using the model to develop a federated view of operational risk among a collection of related entities. So that's an interesting use of the model.

And what have I missed? Oh, I know of an organization that has just begun to use the model. And their interest Julia is on establishing a baseline of return on investment for the organization's expenditures related to resilience activities. And that one given what I know about the model, it certainly makes sense as a use for the model. But I was kind of surprised actually to see somebody pick it up with a lot of energy around that important issue.

Part 3: Making the Business Case

Julia Allen: As I listen to you talk Dave, it causes me to reflect on the next question I want to ask Rich. Because you've really laid the stage nicely by talking about the variety of ways in which the model can be used. It's a reference model and people can pick and choose and scope and zero in on their particular areas of interest.

So Rich, my next question for you is around making the business case. And maybe one of the aspects of that is this flexible if you will, if you'll allow me agile use of the model, for using RMM. So typically making the business case for introducing something like a new process improvement model is really a hard sell. There's all kinds of competition for attention and resources. So when you're introducing the model to an organization, what compelling arguments do you use to get them to give it a hard look?

Rich Caralli: So I think I've got the hard question here. But as you both know me well, I'm never at a loss for an answer. So I will give you my answer to this. But I think part of it stems on what you just said Julia. And that is we purposely built the model in a way that would not preclude an organization from making the tiniest investment in the model.

In other words, you don't have to take all 26 process areas, and you don't have to absorb 1000 pages of background and theory and concepts and practice to get immediate use out of the model. You can just simply look at an area of pain, like incident management. You can go to the model and you can see essentially a generic process, culled out of very high maturity organizations who have performed very well in terms of resilience, and you can very quickly assimilate knowledge that took them many, many years, and many thousands, and maybe even millions of dollars to get to.

So that to me is one of the lowest hurdles to entry to the model and it's probably one of the biggest payoffs. You could simply really read a chapter in the book on incident management and say, "How closely does the process that we use in our operational units align with this?" And really get some benefit literally in eight hours.

But I'm also conscious of the fact that the adoption of all models and process improvement approaches really require a stimulus for change. And that stimulus can often be financial. It may be because you want to improve sales or reduce cost or be more efficient. And resilience plays a big part in all of that. Yes, it will take an investment to take on the adoption of the model or to catalyze process improvement. But in the end it should have some payoff.

The principle we used when we developed CERT-RMM was the same as CMMI, that essentially and I'm using air quotes “quality is free,” based on the famous book by Philip Crosby. The assertion in that book, and in that use of a maturity model that's in that book, is that when the organization does the right thing and implements practices that assure high quality in its products, the investment they make in this quality activity should pay for themselves.

So as we translated those concepts to the resilience challenge, the same should hold true that by improving the processes the organization uses to manage resilience, it should also be able to improve effectiveness in dealing with stressful times, reduce redundancy of effort (which is a huge issue in organizations, particularly if they silo the security and continuity and IT operations activities,) and to avoid costly impact. And that is often the big driver for improving. It's the thing that you're going to avoid that really has payoff.

All of these things can be quantified by an organization to make an adoption business case. And in the end the organization is already making a considerable investment in IT, security, and resilience. Wouldn't it want to ensure that this investment brings the best return possible?

From anecdotal evidence, I would say that CERT-RMM can be used as a guide that the organization can use to improve the effectiveness of these activities and definitely make them more efficient.

Julia Allen: Okay, okay. I'm going to buy one. It sounds good to me.

Rich Caralli: Good.

Part 4: Getting Started; Upcoming CERT-RMM Products

Julia Allen: Okay, so we've talked about the model. We've set the stage, why we're using it, talked a little bit about how it's structured, how some of our customers are using it. So let's say, like I just said, let's say I buy all that.

So Dave, but there's taking it one bite at a time there's getting started. So in your experience in working with customers and again in your own observations, where do you think is the best place to start? If I wanted to dive into the model and pick like Rich used the example of incident management where should I start? What should I do first? Get me through the first couple of steps.

Dave White: I spend a lot of time teaching our Intro course, and so I get to talk to people about this issue a lot. “Okay, now we've covered these 26 process areas, now what?” How in the world do you pick where to start? And it's interesting in the course that most people who sit there and listen from the perspective of their own organization, by the time you cover those 26 process areas over a day and a half or two days in the course, they know where they want to start, right? Because they're listening from their organization. And that's actually, for people who take the course or don't take the course, that is what I recommend. Sit down and peruse the model, which is easy to do.

Each process area has a purpose statement, which is just one or two sentences long. And you can read those 26 sentences, and get a sense for what the 26 process areas are about, and very quickly whittle down that set of 26 to a subset that you'd like to start with based on the objective that you have for improvement.

So the first step is scoping. And part of the scoping equation is to pick which parts of the organization you're going to work on, and another part of scoping is to pick which parts of the model you're going to use. And those need to be aligned around some organizational objective and around the sponsorship for your improvement activity.

So we always encourage people to pick a part of the organization and a part of the model that aligns well with both the objective for undertaking improvement and the span of control or influence of the sponsor you have for the improvement activity. And if you haven't convinced somebody other than yourself that improvement is needed, then take a look at your own span of control and your own span of influence and figure out what it is that you, what part of the model you can use to make improvement in that part of the organization. So that's the first step.

You could use just one of those 26 process areas, or you could use parts of one or a handful of process areas. If there are specific goals or specific practices within those process areas that speak to you and speak to your improvement needs, then you can certainly start there.

So that's what we recommend. We don't have a prescribed starting point. And in the organizations I've worked with, I've seen a lot of variation really based on their objectives for the improvement activities. So the good news is with this model you do get to pick and choose and you can use as little of it or as much of it as you'd like.

Julia Allen: Are you finding Dave, that there are particular roles inside the organization like the person responsible for business continuity or the chief information officer or the chief information security officer or perhaps some cross-organizational Team are you finding any consistency in the roles that have interest in a model such as RMM?

Dave White: Well certainly the roles that you mentioned are people that we've seen express interest in the model, and in fact sponsor improvement activities associated with the model. Rich, you may have some additional profiles of people that you've seen.

Rich Caralli: Well I think it's been interesting, the cross-section that we get. And it really depends on what brings you to the class or what brings you to the model. But for example Julia, one of the things that you know because you've talked to so many senior executives is, we had several people in classes who said, "Look, I'm the CIO in a large organization" or "I'm the CISO, and it's no longer acceptable for me to go to the board of directors (or whoever provides governance over the process), and say when they ask the question, ‘Are we secure, are we resilient?', we answer the question by saying, ‘Well nothing's happened.’ It's no longer acceptable to do that. So I have to have something that I can have more justifiable confidence in, to express as an indicator of our success; as an indicator that we're spending our dollars in the right places; as an indicator that we're actually getting benefit out of the practices that we're implementing." Maybe we're a COBIT shop but are we seeing any benefit from that?

CERT-RMM can give you a way to say, "Yes, we actually are seeing benefit from implementing COBIT and its bringing cost savings or it's making us more secure." So certainly that CxO level is really interested here. But I think you can also go down to the people who are really in there with sleeves rolled up doing the work because they're feeling the direct pain. So they're looking at processes and I go back to incident management again. They're seeing the same incidents over and over again. “Why are we still dealing with these things?”

We've had people come to CERT and say, "You know, we've followed all the standards, and we keep having data breaches. So what's going on? We're following the standard." And we're saying to them, "That's because you're not getting to the root cause, and that's your area of pain and somehow you're not getting there." So we have people down in the trenches saying, "Well what can help us ferret that out?" Because clearly just by using a code of practice or complying with some standard is not causing that problem to go away.

So I have to agree with Dave. When you teach a CERT-RMM course, it's really interesting the cross-section you're going to get in there. Because its people who are business people concerned with the endgame are their services mission assured? Its people who are in what we call the resilience disciplines: security people, continuity people, IT ops people. But it's also the governance and management people who are looking over all of this and saying, "How can I best characterize how well we're doing?" It's very difficult to characterize a posture, and CERT-RMM gives them a way to finally do that.

Julia Allen: Great. So Rich, as we come to our close obviously we're at the beginning of this magnificent journey. So could you say a little bit about what's next for RMM and perhaps some resources where our listeners can learn more if they're interested?

Rich Caralli: Sure. Well I'm actually glad you said that. Because I think even with all of the work that we did, I would say we've still only scratched the surface. It's great to have a model and it's great to have a book and those things but I think we're really starting to see the value of what we've invested in. And we have a lot of implementation artifacts coming down the pike in the next year.

As you mentioned earlier Julia, version 1.1 of the model will be released in a new book published by Addison-Wesley. It's got some implementation guidelines in it. It answers some of the questions that Dave and I have been discussing here on the podcast as well about where to get started, and how to use things like targeted improvement roadmaps, which is a way for you to figure out what are the three or four key process areas in the model that I should start with. So we give you some guidance to do those things.

I've mentioned this cross-walking a couple of times in this call. What I mean by that is we took a lot of the standard codes of practices that organizations use every day in security and continuity and IT ops, and we've cross-walked them to the process areas in RMM. Well that's very valuable for organizations that want to elevate their practice-focused approach to a process approach so they can start institutionalizing these processes.

That's really the first step. If you really want to get a high maturity in this space, you have to leave a practice mindset and elevate that to a process mindset. And the CERT-RMM Code of Practice Cross-Walk, which is in a v0.95 version right now, will be updated in the next year. It will include cross-walking to common NIST practices. So our friends in the federal-civilian agencies and the federal government will be able to make better use it. And we're also planning to map it to the DIACAP process for information assurance in the DoD context. So we'll have usability of the model in both of those spaces.

I also wanted to mention that we'll begin our licensing activities around the model. Most frequently you hear about appraisal. We follow a similar structure in the CMMI in that we offer class A, B, and C appraisals. And we are starting to license appraisers and team members on appraisal teams.

We also have two exciting other roles that you're going to see in CERT-RMM. One is the CERT-RMM Coach, which is a person who helps an organization use the model to really get improvement, to really make a difference. So they're less concerned about the appraisal activity. They're really on the other side of that, using the CERT-RMM as a body of knowledge.

We are also getting ready to publish the official capability appraisal methodology, which describes how you do a CERT-RMM appraisal using CERT-RMM as the base model. We'll be offering new course work in the next year to support fast-tracking appraisers in the CMMI community to get credentials in the CERT-RMM community. And we'll probably be offering an apprentice program where we take people under our wing and put them to provisional certification, to do appraisals in a very short period of time. In fact, we're looking for organizations that are interested in doing that.

One of the best ways to get a model like this to stick is to do it from the inside not having us come into the organization every time you need to use the model but training people inside your own organization to be the model experts and to use the model in a repeatable way. That's the best way to build an installed base.

If I can go another minute Julia, We kicked off a new area of work, one that you're very familiar with, called resilience measurement and analysis. I think this is one of the most exciting things to come out of the CERT-RMM work because and I can summarize it by saying, "Why do this?" Well, in the end what we want to know is that improving resilience processes has actually made the organization more resilient. Everybody wants to know that. And so that I think will feed into the business case, once we start to get some of those measurements that can actually tell us that we've moved the bar, that we've actually done something that pushes the organization in the right direction.

As you know, we published a technical note on that this year that's available at the SEI website. We're using CERT-RMM in the critical infrastructure protection space. We're looking at applying it in the healthcare field around the protection of electronic health records.

We're also working with a large hospital system to start thinking about how can CERT-RMM be moved back into the early lifecycle to catalyze the software and systems resilience 'build it in' approach and give a context or a framework for doing that. So those are all exciting things.

We're also looking at ways to have organizations use CERT-RMM and CMMI-for-Services in a specific context. As you know, the services model is about developing a high quality service delivery management system. When you overlay CERT-RMM on top of that, you get high quality, resilient Services, which in the end is what organizations want.

And if I could just mention one other thing. The CERT-RMM Navigator role is paired up with what we call the CERT-RMM Compass. So we've come to the realization in the past year that a formal appraisal might be a high barrier to entry into a model for many of our adopters. So we're in the process of creating a self-administered Compass survey that allows organizations to get a health check using the model. And it gives them the range of experience of the model. It doesn't go real deep but it gets them started.

So it can catalyze a longer process improvement approach, with a very low initial investment. The CERT-RMM Navigator role is somebody who facilitates that assessment and we're beginning in the next couple of months to roll out both of those exciting pieces of work.

Julia Allen: Well we definitely have a lot on our plates. I don't think any of us have to be concerned about our day jobs for sure. And I really do appreciate Rich very much your time today in walking us through the model and your leadership in keeping this effort going. So thank you so much.

Rich Caralli: Thank you Julia. I'd just like to point the listeners to our website, where you can see the latest of these artifacts, the cert.org website. And of course with our friends at Addison-Wesley, the publication of the CERT book as part of the CERT Series, the CERT-RMM book Version 1.1, in November. That's an exciting milestone for us.

Julia Allen: And Dave thank you Rich and Dave I'd really like to thank you as well for your leadership and all the work that you're doing in the field to make sure that this has practical, tangible, measurable results in the field. So thank you for your time today.

Dave White: Thank you Julia. You're welcome.