Insights from the First CERT Resilience Management Model Users Group Transcript

Part 1: Members, Preparation, Scoping

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 principal researcher at CERT, working on operational resilience and software assurance.

Today I'm really pleased to welcome back my colleague, Lisa Young. Lisa is a senior engineer with CERT's Cyber Resilience Center. And today Lisa and I will be discussing our experiences with the first CERT Resilience Management Model Users Group Workshop. We refer to it as the RUG. And I was Lisa's co-leader for this workshop. So I may chime in from time to time, in addition to asking Lisa the questions about our workshop.

So for our listeners who are unfamiliar with RMM, the Resilience Management Model, as a background we've posted a number of podcasts and webinars on the model. They're available on the CERT RMM website; and we encourage you to give those a listen for background. But we're going to talk about the Users Group today.

So welcome back, Lisa, really glad to have you on the Podcast Series again.

Lisa Young: Thank you Julia. I'm really happy to be here.

Julia Allen: So just to set a little bit of background -- we have the model. It's been out there since 2010/2011. So why did CERT decide to offer the RMM Users Group Workshop? And a little bit about the background and maybe a little bit about how it's structured.

Lisa Young: Sure. So when folks look at the CERT RMM book, and the model, they see a thousand pages of text and it's often overwhelming. And one of the things that we often get questioned about is: "How do I actually use the model? How do I implement the model? What do I do with the model? How do I use it to make myself more resilient?"

So the RMM User Group Workshop was structured as a way for organizations to come to us with a business problem and implement a set or a specific set of model practices that would help them improve in that area.

The workshop is structured over the period of time of approximately 12 months. And it's structured in a series of two-day workshops, generally one per quarter. And it brings together generally four to five organizations, with two to three participants each is an optimal number, to share information, work on a business problem, and use the model in real implementation in operations.

Julia Allen: Okay. So the idea is really to give folks more of a hands-on experience of applying the model to a specific problem that they have, right?

Lisa Young: Yes definitely.

Copyright 2012 by Carnegie Mellon University

Julia Allen: Okay, so let's talk about the first workshop because that provides lots of rich examples for our discussion today. So what organizations did participate with us in the first workshop series? I think folks will be interested in the diversity of member participants.

Lisa Young: Definitely. So, a couple of things. The first thing we did to solicit participation was ask our current customers and people that we were already working with. So we had three organizations. The first one was Discover Financial; the second one was Lockheed Martin, two specific areas of Lockheed Martin; and the United States Postal Inspection Service were our first three candidates and our first three members.

We added two members later on. The Carnegie Mellon Information Security Office, we had been working with them separately, and asked them to join the user group. And also our own team, the CERT Resilience Enterprise Management Team. We decided that if we were going to help people to use the model, then we should probably use the model ourselves on an improvement objective that we set.
One of the things we did to prepare the participants is we asked them to come to the first workshop having taken the CERT Introduction to CERT Resilience Management Model course. We also interviewed them to understand their expectations. And also we asked them to bring us a business problem to solve -- not a problem based on the model -- problem that they perhaps were having in the areas of resilience; resilience meaning business continuity, disaster recovery, information security, physical security, incident handling, IT operations. So to bring us a business problem that we could help them solve using the model in about 12 months.

Julia Allen: Yes, and I remember as you and I participated in this pre- interview or pre-workshop interview process with each of the candidate member organizations, one of the things that I really liked about that was that we could tailor the workshop series to the needs and the interests of the participating members. So we looked for commonality, in terms of what they wanted to get out of the workshop series, and were able to actually custom tailor the workshop to meet those expectations, right?

Lisa Young: Yes absolutely. And I think that provided a lot of value for them. And even with the diversity of the participants, it was amazing how many common characteristics and problems that they actually had as a group -- particularly in responding to events or incidents in their organizations; working with supply chain partners; or looking at their external providers.

So there was a lot of things that they brought to the table that were similar, even though they had different business objectives and different missions.

Julia Allen: Great. So as we got ready and started preparing for Workshop 1 -- can you say a little bit about what we did at Workshop 1; how we set the stage; how we got them ready to actually start to engage with the material and address their particular business problem?

Lisa Young: Well, we spent a good bit of time on understanding model scope; understanding which parts of the model would fit best with the problem that they were trying to solve. And we also spent a good bit of time on scoping the span of control of the sponsors. So one of the things that is important about any improvement objective is to have sponsorship.

And in the first workshop we spent a good bit of time on honing the practices from the model that would be important to them; and also the sponsor's span of control -- what realistically could an organization expect to get done, that was in their span of control, in the period of time

Copyright 2012 by Carnegie Mellon University

that we had laid out for that? So we spent a good bit of time on model scoping, organizational scoping; where to apply the model in the organization, which parts of the business?

And we also spent a good bit of time on diagnosis. What kind of diagnosis would an organization want to use? Would it be something along the lines of a very in-depth, evidentiary appraisal, where we collected evidence to look at practices? Or would it be something more lightweight; sort of like our Compass instrument, which is more of a quick health check. So what kind of diagnosis would an organization want to use to gather or gain what their current state was in the selected practices from the model?

Julia Allen: Yes, and I remember some of the discussions; this whole notion of -- let's talk about model scope first -- this whole notion of model scope. I think people often would come in to the model and want to tackle -- there are 26 process areas and they'd want to tackle maybe half of those. And I remember your regularly advising them to make the scope as narrow, the model scope as narrow as possible, right? So could you say a little bit about some of the pitfalls of going too big too soon?

Lisa Young: Yes absolutely. So as a reminder to our listeners, the model does have 26 process areas. And all of the process areas are in the model for a reason, meaning they're all connected in some way or another to developing and creating a more resilient organization. So oftentimes someone will read the book or read the introduction to the book and they'll say, "Okay, I want some of that resilience. So give me all the process areas in the model." And as you said, I reminded them that that was too big.

One of the things that's important about model scoping is to choose the areas where you can make an impact. So where it's under your span of control, or your sponsor's span of control, and that you can make visible, lasting changes that will improve even just one thing.

So I'll give you an example. One of the participants was looking at incident handling. And incident, the incident handling process area has about 15 practices in it. And I said, "Well which one of those practices is giving you the most problem?" And they said, "Well escalation of incidents. We don't have a clear process for escalation, and when to escalate, and who to escalate and that's causing us problems." I said, "Okay then just pick one practice out of the model -- escalation of incidents -- and focus on improving that one." And so definitely model scoping is a challenge for organizations. And they often want some of everything that's in the model.

Julia Allen: Right, the old walk before you run. And similarly on organizational scoping and the span of control of the sponsor -- as I reflect back on our experiences those people or those members in the room who defined an organizational scope that was within their own span of control, the members of the user group, where they could go back to the organization and they actually had the authority and the role and the responsibility to make change happen in a particular arena, if they picked an organizational scope that matched their own span of control, I believe we observed that they were generally more successful, right?

Lisa Young: Yes definitely. That's a good point.

Part 2: Diagnosis, Process Definition, Measurement

Julia Allen: Okay. So let's talk about Workshop 2 a little bit. So we've set the stage, got them to think about how big of a bite of this elephant that they wanted to take, and apply it to what

Copyright 2012 by Carnegie Mellon University

problem they had -- because I know we were always refining their improvement objective as well.

So can you say a little bit more, maybe do a little bit deeper dive on diagnosis? Because that's really where we focused on Workshop 2 -- getting ready for them to actually go do their own diagnosis between Workshops 2 and 3.

Lisa Young: Definitely. So, one of the things that, as I said before, the members needed to understand was what kind of diagnosis they would like to perform in their own organization. Some organizations at the table were new to model adoption. They were new to process improvement. They didn't necessarily have a structure in their organization for diagnosing resilience practices.

For those organizations we advised them to perhaps hitch this to something that was already in place. For example, if you have a compliance process and you use the compliance process to check evidence of controls, you use the compliance process to collect documentation. Perhaps your diagnosis could be right alongside that. You could hitch your resilience practices to your compliance efforts.

Other organizations, they had a much more mature process group or process improvement group; or perhaps they were, they used Six Sigma or Lean. And they had a group who's responsible for improving, diagnosing and improving processes. In those organizations they were able to use the resilience practices in an existing area already, in an existing process improvement group.

So when performing a diagnostic, it's important to understand what information that you're trying to get, to use the model to uncover the ground truth, so to speak. And so it's important to have a wide range of objectives, as you're collecting the diagnostic data. And that you talk to a variety of people that will give you feedback on whether or not these practices are actually implemented in the organization.

Julia Allen: So can you say a little bit about Compass? Because I know we introduced each of the members to a variety of diagnostic approaches, including ones that they may already have in place and just want to piggyback on. But as I recall, most of them decided to take some subset of the Compass survey -- it's a survey- based questionnaire -- and apply it to their data collection activity. So can you say a little bit more about how that was used?

Lisa Young: Sure. So in the history of the SEI, we have this thing called the SCAMPI Appraisal Method. And it's very evidence-based. And there are different classes of it. But generally speaking it's a large diagnostic effort, meaning it takes a lot of preparation and it takes a lot of feet on the ground to actually execute.

One of the things that we wanted to do with the model to make it more adoptable is to have an assessment method where an organization could get a quick health check of what their resilience practices look like and without a lot of evidentiary data collection.

So the Compass is our -- what I would characterize as a lightweight health check method that's based -- diagnostic method -- that's based on the model. And it's a set of questions and answers. So people will read a practice statement and then answer the -- choose the answer that best fits how they're currently performing a practice. And from that they can get a sense of perhaps where they'd like to focus more closely in an organization, on a diagnostic; or maybe a deeper dive on a particular practice.

Copyright 2012 by Carnegie Mellon University

Julia Allen: Great. Thank you. So there was a lot that happened between Workshop 2 and 3. I think that was -- we had a pretty significant chunk of time and we did some telephone check-ins with folks to see if they needed help along the way. So as we came into Workshop 3, they had a refined improvement objective; maybe a refined organizational scope or refined model scope, and some diagnostic results.

So for our listeners' benefit, can you describe what we actually did with all that rich data and understanding in Workshop 3?

Lisa Young: Sure. So one of the focuses in Workshop 3 was process definition and measurement. And even though we had collected a lot of data, organizations were still struggling with this notion of "Why is it important that I have a defined process? And how do I, if I have a process that's undefined, how do I define it? And what is the benefit of defining a process?" I think that was really a big ah-ha moment for a lot of folks, is they had been assessing their practices in a variety of areas. But this notion of defining a process was foreign to some of them.

And it does take time and energy to define a process. But some of the benefits of defining a process is that you have a standard repeatable way to carry out, for example, incident escalation. So you have a defined process for doing that. Everyone knows what the process is and everyone can do the process.

What's also really important about having a defined process is that it allows you to have measurement points. So somewhere in the process that you've defined, you can take measures. And the measures allow you to collect data and then understand if you're improving over time. So it sets the stage for building and putting into place a measurement program.

Julia Allen: I remember some of my ah-ha moments as we were heading into Workshop 3 and I was working with you and others on the process definition and measurement work. Because I kept thinking -- we have the model; we have these 26 process areas. They lay it out in fairly good detail what you need to do. But I think what we discovered along the way -- and we've discovered this certainly working with our customers -- that the model is really the 'what'; it's not the 'how.'

Lisa Young: That's right.

Julia Allen: So let's stay with your example of escalation. So it (the model) talks about making sure you escalate incidents to key primary stakeholders. And but the question is how does that actually happen? As you said, feet on the ground, actions taken, what happens first, what happens second, what happens third? And that's really the reason for coming up with an implementation-level defined process, right?

Lisa Young: Yes absolutely. So especially in the case of incidents, for example, there's a lot of risk associated with different staff members performing the process differently, right? So if you have a standard process that everyone knows what the process is and everyone can follow the process, it makes this notion of responding to incidents, for example, a lot more real. And it keeps you from running around with your hair on fire.

So oftentimes organizations will experience an incident. They hadn't really thought about how to handle the incident before it happened. So they run around and perhaps may make some mistakes or do things differently or not collect the evidence that they need for law enforcement

Copyright 2012 by Carnegie Mellon University

or for insurance purposes. So there are many reasons for pre- planning a response to an incident, which means you have a defined incident response process.

Julia Allen: Right; and additionally collecting the lessons learned from key incidents so that you don't, you're not set up to repeat those again in the future, right?

Lisa Young: Yes definitely. And understanding -- so one of the, one of the problems that we see a lot in organizations, that the model can help solve, is this notion of "is this incident caused by a vulnerability that I should've already known about and handled?" Right? So there's often a disconnect between the vulnerability management staff and the incident management staff.

So using the model to understand lessons learned from how you handle incidents will point to whether or not you need to shore up your vulnerability management process. So, as I said before, all of the process areas are in the model because they improve organizational resilience. But getting to what are the specific problems that are subjective to one organization, and helping them pick the practices that will make the most impact, I think was the thing that I liked best about the workshop.

Julia Allen: So that's an interesting point. And I know we struggled with this a little bit because it's so organization and problem specific.

Lisa Young: Yes.

Julia Allen: But as members came in with their diagnostic results, can you say a little bit about thinking about how to prioritize; how to pick the high impact, high visibility, maybe the most critical pain point areas that came out of the diagnosis to focus their action planning on?

Lisa Young: So when the organizations came in with their diagnostic results, we wanted to help them prioritize which of the problems they uncovered was most impactful. And part of the criteria that we used for doing that was -- number one was sponsorship and span of control. So do you have span of control for this particular pain point that you've uncovered in the diagnostic area?

The other thing is, is it important to understand the current process that you have in place and why it's not working for you? Is this a process that is highly repeatable? -- meaning that it happens all over the organization; therefore you'd gain a lot of value from improving it.

Julia Allen: Right, and it would have some lifespan to it, right?

Lisa Young: It would have some lifespan, yes.

Julia Allen: Right, so if you invest in defining the process, you're going to get to reuse that artifact and keep improving it over a pretty good chunk of time.

Lisa Young: Right, and one of the other criteria that we used to help them understand whether or not this would be useful for them is -- is the process, does the process need to be done -- does the action and the task and activity that make up the process -- does it have to be done in exactly the same way every time to be effective for the business?

Copyright 2012 by Carnegie Mellon University

And so even if it's done infrequently, if it's a process that needs to be done exactly the same way, executed consistently by all who perform it, that was another way that we helped them prioritize the value of the process definition and improvement in their organization.

Julia Allen: Right, so I remember an example of that one was configuring a laptop, a desktop, a server, and making sure that's done the same way every time, right?

Lisa Young: Yes, absolutely.

Part 3: Lessons Learned and Workshop Improvements

Julia Allen: Okay. So off they went, after Workshop 3, with an idea of where they actually wanted to take improvement actions. So we drive to Workshop 4, which is the culmination of the series. And can you say a little bit about what kind of feedback we got and what progress each of the members made coming into Workshop 4?

Lisa Young: Sure. So by this time, nearly a year had passed. So remember this is an iterative process over time. And one thing that I forgot to say before is that our job -- Julia and my job, and the team's job -- was to facilitate use and implementation of the model. But the folks around the table, the workshop participants, were actually the ones who did the work, right? So they went back to their organization. They took what we taught them and they used it in their organization. And then came back to each workshop to see how had they done and had it made a difference in their organization?

So by the time we got to the last workshop, members gave us some feedback on what worked and what didn't work -- specifically from a diagnosis perspective, from a process definition perspective, from a sponsorship perspective. But they also had a better understanding of the model itself and how to implement it. And so now they had “the what to do,” which is in the model. They had a “how to do it” and they could then apply that to any other business problem that they were having.

The other thing that was important is that for the organizations that already had a mature process group or a process improvement group in their organization, it expanded their scope of things that they could improve. So, for example, if they were traditional software systems engineering improvement -- if that was their area of focus -- the model gave them a way to apply those constructs that they already knew to information security, business continuity, disaster recovery, IT operations.

Julia Allen: Right, and I remember from our own improvement project -- as you said at the top of our podcast, we applied all of this structure and guidance to our own internal improvement project.

I recall just how really difficult that was, to pick and choose the right model scope, the right organizational scope, the right problem to make it broad enough to be a problem worth solving but to make it narrow enough to be where you could actually put true implementation action in place and have it stick.

And so it's -- it did have quite a few challenges to it. And I recall in Workshop 4 that we had a chance to elicit a lot of feedback on what worked well and what didn't, to help us improve future workshops, right?

Copyright 2012 by Carnegie Mellon University

Lisa Young: Yes definitely. And we made -- in our own improvement project, in our own organization, I feel good about the changes that were made as a result of our diagnostic effort. And some things that we did internally to change some of our procedures -- for example, in explicitly, in our policy, explicitly stating how often things were backed up and how comprehensively data was backed up.

So even in our own policy, I feel good about the changes that we made that were implemented. But it was difficult to do. And one of the ways that we handled that, if you remember, was to get our own house in order -- for example, our own, just our own small group with our own sponsor in order, before we then took it to other areas and other departments within CERT.

Julia Allen: Right, and the other thing that was helpful is it gave us insight to be -- to lead the members in the Users Group to try and develop artifacts and guidance and ideas. So our improvement project led theirs by maybe 30, 60, 90 days. So by the time we got to the workshop where we were going to suggest to them what actions to take next, we'd already taken those for a trial run with our own improvement project.

Lisa Young: Yes. That was very helpful.

Julia Allen: Well, Lisa, this has been great and I think an excellent summary to help our listeners understand how to take the next step with the model. So do you have some places where our listeners can learn more?

Lisa Young: Yes. They should definitely look at the website. There are also several technical notes on the RMM Users Group but also on the measurement and process definition. I think those are very useful in helping organizations understand why they might want to take a look at their current processes, and are they well defined and well scoped? And does everyone know about them and are they repeatable?

Julia Allen: Excellent. And we'll put links to all of those in the show notes. Well thank you again, Lisa, for your time today; for your leadership with the workshop series. I think we had a blast working on it together; and I appreciate your time on the podcast today.

Lisa Young: Well I could not have done it without you Julia and I could not have done it without all of our wonderful participants. So, just a big thank you to them. I think I learned as much as they did.

Copyright 2012 by Carnegie Mellon University