US Postal Inspection Service Use of the CERT Resilience Management Model
Transcript

Part 1: Motivation for Using RMM – Process vs. Controls

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.

I'm very pleased today to welcome Greg Crabb. Greg is Inspector in Charge of Revenue, Product, and Global Security for the United States Postal Inspection Service. And Greg and I will be discussing his organization's use of the CERT Resilience Management Model, which we refer to as RMM. In addition, CERT is doing work for Greg's organization, and I am a member of that project team.

For our listeners, for a little bit of background, if you're unfamiliar with RMM, we've posted a number of podcasts and webinars on the model and those are all available at the CERT RMM website.

So with no further ado, welcome Greg. We're really glad to have you on the podcast series today.

Greg Crabb: I'm excited to be here as well. Thank you.

Julia Allen: So you have been a user and advocate of RMM for several years, and I'm just curious as to how you initially found out about the model, and what about it grabbed your attention?

Greg Crabb: The Postal Inspection Service has been working with Carnegie Mellon for the last several years. And several of the researchers recommended that we understand more about RMM, to improve our processes for investigative response to network security incidents.

And in studying the model, I learned how it could be applied to other resilience and investigative activities of the Postal Inspection Service.

Julia Allen: So when you talk about resilience, what does that word mean to you? What does it connote?

Greg Crabb: So resilience means being able to respond to any threat or incident or situation that can be posed against a particular asset. And the Postal Inspection Service provides investigative response to a variety of incidents from hurricanes and the impact that they have on Post Office operations, to carrier robberies or thefts where our employees are threatened, and a myriad of other resilience activities that we need to manage.

Julia Allen: Excellent, thank you. So what are some of the challenges you face -- you've mentioned several -- in your role in particular, for which you've observed, or in your application of RMM you've found that it does offer value? What are some of those big challenges?

Greg Crabb: So I wear three hats for the organization. I'm responsible for our revenue investigations, our product security work, and also our global security work within the Postal Service.

For our revenue, I'm responsible for assuring proper payment of $64 billion dollars' worth of annual revenue to the Postal Service from our mailers. I'm also, under my product security hat, I'm responsible for the delivery of our letter and package products, from a security perspective.

And I manage the operational security needs for our international business. And I'm using RMM to assure structure and completeness in our organizational process management over those activities.

Julia Allen: We've seen lots of different approaches to the various disciplines that make up resilience -- information security, business continuity, aspects of IT operations, maybe even a little disaster recovery and crisis management.

So what have you found to be attractive about a process approach, or a process management approach, versus a more traditional control based, or compliance based approach for your areas of concern?

Greg Crabb: I find that, from a business partnership, I can be a better partner to the business owners that are attempting to expand the product base of the Postal Service, meet our customer needs. And in a process approach, as opposed to a controls based approach, I find that by forcing controls upon business organizations, they are very resistant and want to know why they have to meet a particular control. It may work for one product; it doesn't work for another product.

But with a process approach, I can assure that the goals of a particular process area are met without the requirements of a specific control objective. And in doing so, I find that I don't drive as significant of cost structure into products because we can be much more flexible in how we meet those control objectives, as opposed to putting control requirements into a particular product or service.

Part 2: Using RMM to Address Three Diverse USPIS Objectives

Julia Allen: Thank you for that explanation; that's really helpful. So let's talk about some applications because I know you have many initiatives where you've found that there's content within RMM that you've been able to use. So let's say within the last year or so, could you give us a few examples of how you've applied RMM to address some of the challenges that you face?

Greg Crabb: Certainly. I get a lot of value out of looking at RMM from a number of different perspectives and I'll walk through a couple of those.

The first is a new organizational responsibility that I'm taking on in the area of export screening. And on a weekly basis, the Postal Service processes well over a million packages to overseas locations. The organization needs to assure that we meet specific export control requirements, and I have a responsibility of assuring that mailers comply with all of those requirements.

I've relied upon RMM to form the structure of this activity that I'm taking over. Through a project initiation meeting with my staff, we defined key RMM process areas that need to exist and at the specific level of maturity that they need to exist for us to take on this task.

The process areas that I included were human resource management, compliance, organizational training and awareness, measurement, and several others. I was able to use the model to define the specific goals and practices that I needed my staff to achieve, and we were able to build a project plan around those particular areas. The suggested work products that were defined within each practice guided our decision-making on what outputs were necessary to show the completion of the specific practice.

And RMM has allowed us to take a very complex, and some consider overwhelming, task and provide for an appropriate separation of function, managed to a common criteria. It's been really refreshing to the folks that work for me. They understand what they need to do and what goals that they're achieving with each of the work products that they're generating. So it's good for everyone involved.

Julia Allen: Yes, if I may interject something here again, keeping in mind that some of our listeners may not be familiar with the model. RMM has 26 process areas, covering the disciplines we mentioned earlier.

And it's very helpful in using the model because -- in book form, its 1,000 pages that goes thud on the desk and it can be pretty daunting at first exposure. And what I appreciate that you're describing, Greg, is for a specific objective, like in this case, export screening for international mail, you've mentioned, I believe, one, two, three, four process areas as opposed to boiling the ocean and figuring, thinking that you had to address all 26.

So I wanted to point that out to our listeners, that you pick and choose those process areas, and even within a process area, those specific goals and specific practices that are most germane to your objective, and then just don't have to deal with the others, right? Is that what you found, Greg?

Greg Crabb: Absolutely. Scoping the project to the specific need is critical with the use of the model.

Julia Allen: Great. So how about your second application?

Greg Crabb: So recently, I used several process areas to assist my, in my assessment of a new product that the Postal Service was considering. Some would consider it a controversial offering of the Postal Service, so due to its nature, I can't necessarily disclose what the product would be. However, just like any business that contemplates the risk- reward of a new product, RMM can be a very strong tool.

In this particular analysis, scoping and risk considerations were important. I dissected the product offering into its key process areas, as we talked about earlier. For each process area, I applied the RMM Risk Process Area.

More specifically, I focused on developing strong risk statements consistent with the criteria established in a specific goal and practice under, referred to as “identify asset level risks.” By walking through each process, I developed a catalogue of risk statements for the product. I used these risk statements to prepare a briefing for the Chief Financial Officer. In presenting these risk statements, the organization was able to properly define and apply mitigation strategies.

Julia Allen: You said, in a couple of cases -- and I don't know if these two are examples of that -- you've been able to pick up the model, refer to relevant goals and practices and, in fairly short order, frame a scope and frame an approach. Was that true in this case?

Greg Crabb: In this particular situation, the CFO asked on a Thursday, whether I could have a briefing prepared for him on Monday. And instead of boiling the ocean, I went to the model, pulled, extracted those specific process areas that would relate to the product offering, and was able to turn around a very solid presentation to him in basically three days.

And without the model, you don't even know where to start, in my opinion. And the CFO really had a nice presentation on his desk for consideration on risk mitigation strategies.

Julia Allen: Right, so you found that the structure within the Risk Process Area, in particular, gave you the architecture or the foundation for the key messages that you wanted to help him deliver, correct?

Greg Crabb: Absolutely.

Julia Allen: Great. I believe you have one more example for us. I love these applications because I think it makes the model come alive for people, when they hear how it can actually be applied to a real problem. So how about a third one?

Greg Crabb: The last example comes in the area of measurement and monitoring. In the last year, I have guided the development of new measure and monitoring activities for our organizational examination of revenue resilience. As a law enforcement agency, protecting our $64 billion dollars in annual revenue, it's of critical importance.

Through the use of RMM, and developing a professional staff focused on measurement, we've defined a number of performance reporting capabilities to manage the resilience activities that we're responsible for.

Julia Allen: Would it be fair to ask you to give an example of a couple of the key measures, or at least, how you're reporting out for revenue resilience?

Greg Crabb: There are a number of measures that we've developed over the last year that are exciting for our team. The first is a relative risk rating for each of our customers. And by developing this risk rating, we can examine what each organization represents to the Postal Service from a fraud perspective, and if there's opportunities that we can apply procedures to either identify criminal misconduct or whether we can reduce that relative risk by applying appropriate control procedures.

Julia Allen: Excellent.

Part 3: Mail-Specific Process Areas; Appraisal for International Mail

Julia Allen: So we are working with you, under your direction, to develop several mail-specific process areas that are derived from RMM and complimentary with RMM. And I think it would be really helpful for our listeners to have you say a little bit about how you intend to use these mail-specific process areas going forward.

Greg Crabb: This is an exciting project and I really enjoy working with you and your team. By creating four mail-specific process areas, we will be able to leverage the entire RMM model for every resilience activity of the Postal Inspection Service.

Briefly, the process areas involve the transportation, management, and delivery of mail. By defining specific goals and practices that need to be met in these areas, I can define a common criteria for assuring the products of the Postal Service are delivered with resilience at their core, help evaluate business partners and customer operations in their handling of mail, and assess resilience operations for practically everything that the Postal Service does.

Julia Allen: So reflecting on that work, as I believe your intention is to take these mail-specific process areas, but also pull in other process areas from other parts of the model to complement -- for a particular assessment objective or a particular improvement objective. Is that correct?

Greg Crabb: Oh, by all means. The body of work that's been done with the existing 26 process areas is a great resource to leverage. It helps me force multiply. And one of the things that I'm really excited about is by developing and implementing this model throughout the organization, I will be able to communicate with everyone in my organization using a common framework.

And I think having the model, or a model, like this is necessary in order to drive improved performance within the, in my case, the investigative operations but, in most cases, security operations for organizations.

Julia Allen: Great. I know that one of my colleagues, David White, is working with you on an assessment approach with the Universal Postal Union (UPU), and how RMM assessment concepts can be applied to that effort. So I would appreciate your briefly describing what you're doing with the UPU.

Greg Crabb: Oh, certainly. The Universal Postal Union is the United Nations Specialized Agency for postal affairs of 192 postal administrations around the world. Collectively we manage over 600,000 facilities, and deliver to every address around the world.

For the last 16 years, the Postal Inspection Service has chaired the Postal Security Group of the UPU. Through David White's leadership, we've applied the appraisal methodology behind RMM to assess the physical security and aviation screening practices for the international operations of our postal community.

At a Congress in Doha, Qatar in September, the members of the Universal Postal Union will be voting to mandate minimum physical and process security standards. The appraisal methods of RMM will be used to assess postal administrations to these pending mandates.

Julia Allen: So I know you've done some pilots of this assessment method against the draft standard. Can you say a little bit about -- without going into, obviously into specifics -- something about your team's experience, and perhaps some of the insights that you've gained in piloting this new assessment method?

Greg Crabb: We've had the opportunity to use the appraisal methodology at two postal administrations, and the structure of the appraisal methodology was well understood by my team that was conducting the appraisal.
The pre-assessment questionnaires that were provided to the foreign postal administrations were a great feeder product for the time that we were on the ground conducting the

assessment. And the presentation heat map that is generated as a result of the appraisal was understood by every level of management from the security operations personnel that we were assessing to the Chief Executive Officer of one of the postal administrations that we met with.

Julia Allen: Great, great. Well before we close, Greg, I did have one last question for you if you'd be willing to entertain it. So bringing improvement and bringing change and a new way of thinking into an organization, certainly as massive and complex as the Postal Service and the Postal Inspection Service, can be pretty daunting. And you've obviously been a leader and a visionary in this area for your organization.

So what have you found to be perhaps your biggest challenge in socializing the model and bringing it into the Postal Inspection Service and the Postal Service for use? What would be one of your biggest challenges in model adoption?

Greg Crabb: So, to answer that question, I have two lines of thought. One is somewhat amusing around the halls of the Postal Inspection Service and that is the book. Getting professionals to be able to assimilate a book into their work life can be daunting. And it's passing it around and making sure that folks can understand what they're gaining access to through RMM.

The second, and more serious, is applying the RMM model to specific situations that arise -- seeing that the situation can be managed through the use of process areas. And I find that there's -- I'm presented with several situations a week where the model helps me frame the appropriate response that the Postal Inspection Service should apply.

Julia Allen: Right, and in fact you were very gracious in sponsoring several of your subordinates and team members to participate in our first CERT RMM Users Group, which completed last -- at the top of this year.

And one of the things that we laughed about when you talk about the book, is we said “the best approach is to put the book in the drawer.” And then just take the pieces of the model that are applicable to a specific problem and just run with that, as evidenced in the three examples that you shared with us.

And you don't even necessarily need to have the organization know that you're even using RMM. You're just taking the content of it, structuring it, applying it to a problem, and then they turn to you and say “how did you figure that out?” So our little tag line from the Users Group is, “well just put the book in the drawer.” Do you find sometimes that's really helpful, too?

Greg Crabb: Oh, by all means. From a use of the model perspective, in the Inspection Service, my team is pulling out the book and using it. But when we interface with the business units, they have no clue that we're using the model but have a strong appreciation for the work products that we're generating by relying upon it.

Julia Allen: Well thank you for bearing with me on that question, Greg, I appreciate it. So I do have one last question for you -- I always end each podcast with this. So do you have some places where our listeners can learn more, either about your work, or RMM that you might point our listeners to?

Greg Crabb: Oh, of course. If you want to learn more about the Postal Inspection Service, I'd recommend visiting our website or the websites of Carnegie Mellon and the CERT RMM.

Julia Allen: Right, and for our listeners, Greg and I have talked about the RMM book a lot, and I'll include information about that as well in the show notes.

Well, Greg, I can't thank you enough for your time and your preparation, your expertise, and your commitment to finding the value in RMM and applying it for helping you meet your organizational objectives. So thank you so very much for your time today.

Greg Crabb: Oh, and thank you, Julia.