Integrated, Enterprise-Wide Risk Management: NIST 800-39 and CERT-RMM

Transcript

Part 1: Managing Enterprise Risk vs. Chasing Vulnerabilities

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 very pleased to welcome Dr. Ron Ross, with the U.S. National Institute of Standards and Technology sometimes we refer to this as NIST. Ron is also the Implementation Project Leader for FISMA, which is the Federal Information Security Management Act. In addition, I'd also like to welcome my colleague Jim Cebula, a member of CERT's Resilience Enterprise Management Team.

Today, Ron, Jim and I will be discussing how best to organize a robust information security risk management program, a pretty challenging and daunting subject. Ron's organization has described this quite nicely in the recent draft of their Special Publication, 800-39. It's titled *Integrated Enterprise-wide Risk Management: Organization, Mission, and Information System View*.

We'll also be discussing with Jim how CERT's Resilience Management Model, referred to as CERT-RMM, aligns with NIST's work and vice versa. And also for our listeners' benefit, we have posted several podcasts on various aspects of risk management and CERT-RMM, which you may want to check out.

So with no further ado, glad to have you with us, Ron, today.

Ron Ross: Well thanks very much, Julia, it's good to be with you.

Julia Allen: And Jim, thanks for joining us.

Jim Cebula: Thank you, Julia, glad to be here.

Julia Allen: Okay, so obviously the first question goes to Ron, you're up. So I think it's important for our listeners' benefit, to start with some fundamentals.

So when it comes to information security, obviously what we're talking about today, why is managing risk at the strategic enterprise level more effective than a traditional approach of managing risk at the level of an individual system?

Ron Ross: Well, I think you have to go back to look at how enterprises operate today, and we have a 30 year or greater history of actually managing risk at the system level. And I think the first thing that is interesting to note is that senior leaders today have to manage a wide variety of risks, from safety risks to legal risks, to financial. And our Special Publication, 800-39, takes a look at the information security-related risks that primarily come from the operation and use

of information technologies. So we're looking at a very specific narrow band of the risk problem today.

And it's in the context of a very sophisticated threat space today, where adversaries are using very sophisticated tools, techniques, and procedures. Organizations have very important core missions and business functions that they have to carry out. And there is a very high dependence on information technology for business success.

So looking at enterprise-wide risk management, and the security aspects of that, is a very important thing for us to consider in order for us to be successful and carry those missions out successfully.

Julia Allen: Okay, now Jim, this draft report that NIST has put out can be really groundbreaking in terms of raising this perspective. So can you say a little bit about that and how it might tie in with our work?

Jim Cebula: Yes, thanks, Julia. So the 800-39 document I think really is, has potential to be a transformative or groundbreaking, as you say, document here, taking this holistic view of risk management.

Very often what you see is this checklist approach that's built around a list of controls or a control catalogue. And it becomes really a compliance-focused activity down at the system level. And 800-39 is exactly trying to identify and address that issue.

So within the Resilience Management Model, or CERT-RMM, we have this process area called enterprise focus (EF) that really aligns pretty nicely with the top tier guidance that's in 800-39. So in EF we talk about some things like setting the organization strategic objectives, establishing critical success factors, identifying key services, providing governance, providing the financial resources to support these activities.

And it's pretty clear that those are all business issues and senior management level issues that really you need to have a handle on before you get down deep into the level of technical controls that you apply on systems.

Julia Allen: So, Ron, you mentioned this, and Jim laid the groundwork for this. So in 800-39, your Special Publication, you do define a three-tiered approach for risk management. So could you briefly introduce our listeners to each of the tiers and perhaps some of their interconnections?

Ron Ross: Sure, I think it's good to understand the motivation for why we went to the three-tiered approach. And I think this came out of a great frustration after having worked in this field for many decades and continuing to see a focus on chasing one vulnerability after another.

We have a lot of weaknesses and deficiencies that are inherent in some of our information systems and some of the commercial products that we use to build those systems. And the chase for vulnerabilities never ends because the supply of weaknesses and deficiencies is limitless.

And so I think, at this point, the question I wanted to focus on is how do we end up with the systems in our organizations that we end up with? There was no strategy or strategic focus on how do we build and engineer these systems, so we can actually build greater strength or resilience into the systems up front.

And so that prompted us to take a look at the three tiers, where tier one is the governance level or the organization level where you actually define your core missions and business functions. And you prioritize those according to how important they are to your overall mission and business success.

At that governance level is also where a risk management strategy is created, where you look at the types of tools and techniques and procedures that you're going to use to assess risk. And then how do you evaluate risk once you run all those tools and use those techniques?

What is the risk mitigation strategy for the enterprise writ large? In other words, are we going to accept risks or reject certain risks, share, transfer, or mitigate, reduce that risk to an acceptable level? And also at tier one; we have to ask what is our level of risk tolerance? How much risk is too much before we put those core missions in jeopardy and actually jeopardize the ability for the corporation or the federal agency to be successful?

And lastly, at tier one, we ask a very important question today because we have so many things that are changing the hardware, the software, the environment of operations. How do I monitor the risk over time to ensure that with the risks I accepted yesterday are the same as what I'm accepting today? Or if there are differences, how do I deal with those?

And that strategic view, at tier one, then pushes down to tier two and that strategy, then, is used to create a look at our core mission and business processes, the things that we actually execute to carry out those missions.

And that has a very close tie at tier two then to enterprise architecture, which allows us to, in essence, build leaner and meaner enterprise architectures reducing, consolidating, standardizing, optimizing to make sure that we have the most effective IT we can to carry out those missions and then integrating our security requirements into the enterprise architecture at tier two.

And then after we have tiers one and tiers two in place, we now have a roadmap for how we actually build our systems at tier three. We can talk about, as Jim was saying, specific security controls being allocated to various systems, according to how important or sensitive or critical the information is, or assigning or allocating controls to the environment of operations.

So it's a strategic focus all the way down to the tactical, with the strategy informing everything we do down at the tactical level.

Julia Allen: I'm intrigued by this evolution of your thinking because so, as you said in the beginning of your remarks on this question, we start out with the systems. We don't know unknown provenance, how did they come to be? They were, in many instances, just mashed together to meet a particular need.

So given that you've got this huge, current operational and legacy environment in place, if that's your starting point, how have you found that you get organizations to think coherently about tiers one and two when they're so heavily embedded in tier three?

Ron Ross: Well one of the things that we write about in the Special Publication, is this thing called culture. And culture really drives a lot of the way we operate within enterprises. And so some of the things that we're talking about are going to require us to rethink, going way back to how the culture operates within organizations.

It's not something that's going to happen overnight. We have, as you say, a lot of legacy systems that are out there. But unless and until we start to get organized at the strategic level to start asking these very important questions, to include changing how we engineer some of our mission and business processes, to make them more what I call risk aware, that really requires us going back to the current threat space, understanding what the adversaries are capable of, and how vulnerable even our mission and business processes are at tier two.

So it's going to be an evolutionary process. I don't think it's going to happen overnight. But 800-39 is intended to be the first stake in the ground, to get people thinking about an approach that will be much better to get long term health in our security area than we've had in the past.

Part 2: Risk Management and Resilience; Key Stakeholders

Julia Allen: Excellent, well thank you very much for that insight.

So Jim, you mentioned CERT-RMM earlier, and obviously today we're talking about risk management. So what, in our body of work, what do we describe as the relationship between risk management and resilience?

Jim Cebula: Yes, thank you, Julia, that's a great question. So CERT-RMM really is a maturity model for the management of operational resilience. So the model describes an operational resilience management system that has four objectives and several of these tie in really nicely to the comments that Ron just made about risk strategy.

So the four objectives are to: (1) prevent realizing an operational risk to a high value service, so you've got a protection strategy; (2) the ability to sustain the operation of a high value service if a risk is realized, so you have a sustainment strategy; (3) the ability to deal with consequences or get the organization back to a normal state, and then (4) to optimize achieving those things. So with that background, you can describe resilience as being a property of an organization that emerges from the effective management of these operational risks.

And then when we say operational risks, we're very specifically talking about four categories: (1) the actions of people, (2) failures of systems and technology, (3) failed internal processes, and (4) external events. So there's a specific scope there but it is a bigger scope than just systems and technology failures.

And then we also bring together three disciplines that often operate in a siloed or disparate manner within organizations. And that's the security discipline, the IT operations discipline, and the business continuity/disaster recovery discipline try and get those activities all to operate in a converged way.

So in the tier one of 800-39, we have this concept of risk tolerance that Ron mentioned and some of the aspects there are addressed in the risk management process area (RISK) in RMM. But that particular area, I think it deserves mention again because it's so important. Because at all three tiers in the hierarchy, and across all of these disciplines that we mentioned earlier, there are risk management decisions being made routinely whether the organization has any realization of that or not.

So if there's no guidance at an enterprise or organizational level about the organization's risk tolerance and what level of consequence and impact the organization can accept, it's not likely that these decisions are being made in any kind of coordinated or consistent way.

Julia Allen: Great, thank you very much, Jim.

So Ron and Jim, you've both set the stage nicely in terms of framing the problem space that we're discussing today. So let's see if we can get down to some more practical action kinds of questions.

So Ron, as you've talked with organizations and are trying to educate people about the approach in 800-39, who do you identify as some of the key players, participants, and stakeholders that need to really be at the same table and on the same page for establishing an enterprise-wide risk management program?

Ron Ross: Well that's probably one of the most important questions that we can look at today and there are a whole lot of participants and stakeholders in the risk management and information security business within enterprises. But I think, by far, the most important individuals are the senior leaders within organizations. That could be a CEO in the private sector, Chief Financial Officer, Chief Technology Officer. On the federal side, heads of agencies, maybe the second level bureau chiefs.

If you don't have the senior leader involvement, there really is no commitment to making what 800-39 talks about as a fundamental change in how the organization operates with regard to risk management and information security.

That senior leadership commitment is essential toward moving the organization forward. And then, obviously after the senior leadership is onboard, your CIO and Chief Information Security Officers those folks play a very fundamental role.

Procurement Officers what we're trying to do with the three tiers are influence investment decisions and the design of the systems that you actually use to carry out your core missions and business processes.

So at some point, all of those architectural decisions and all of those security requirements have to be effectively conveyed to procurement officials who, in many cases, are not IT experts or not security experts or risk managers. So we have to have very effective ways of communicating with the procurement office.

System developers the folks who build commercial products. Looking at the way the federal government is trying to protect its systems, trying to build better functionality into those commercial products that we can then use in the integration mode to build more secure systems.

And then last, but certainly not least, are the operators on the front lines who are observing the threats. They're observing some of the cyber attacks that we are seeing, responding to those cyber attacks and trying to make improvements, continuous improvements, in the system and applying additional controls where we see maybe advanced persistent threats that are emerging.

And certainly the assessors and auditors can use the basic material in 800-39 to do a better job at understanding where we actually stand with regard to the security state of our enterprises and our systems, to help us move forward in a more productive way.

Part 3: Risk Management Process: Focus on the Red Zone; Getting Started

Julia Allen: Okay, so let's say you've got everybody at the table, you've got your senior leadership on board, they're set to go, but they need clearly they need something to execute. So I think, in your report, you do a great job at describing the four components that make up a risk management process. So can you walk us through that as a way to get people into action?

Ron Ross: Sure, the three tiers that we talked about tier one, two and three, being the organization, mission/business process, and then system level we also define in chapter three a risk management process, which has four classic steps to it as you described.

And before I go into those, I just want to frame the context of why we went to these four steps and the importance of applying those across all three tiers.

I'm going to use an analogy since I think you guys are in Steeler country up there near Pittsburgh. And in football, there's a term called the red zone. It's the final 20 yards on the football field before you go into the end zone.

Up to this point in time, most of our work has been using best practices to try to take care of 80 percent of those cyber attacks that can actually exploit vulnerabilities in our systems to cause mission impact.

But really, with the sophistication of the threat out there today, the advanced persistent threat, we really have to go beyond those 80 percent and look for what I call the red zone security, those 20 percent that can really bring organizations to their knees. This could be a power plant in a small town in the United States, or it could be a manufacturing plant, or it could be a federal agency.

So we start out with the very first part of our risk management is called framing the risk. Every organization has a context in how they make their risk-based decisions. And the framing component, where you establish the context, looks at certain things that certain assumptions that the organization makes about how they're going to be managing risks, what kind of tools and techniques they might be using.

They'll also talk about certain constraints on the risk management process, maybe budgetary constraints, or maybe operational constraints that have to be considered. It's the risk framing component that also talks about how do we establish our risk tolerance within the organization. How much risk is too much before we, again, have a potential adverse impact on our core missions and business operations?

And then, finally, we have to make prioritizations of all of the activities that we're doing and establish tradeoffs where we have to. And that framing step is critical then to going into our cyclic three steps in the risk management process, where we first assess risk. This looks at the classic four components of risk assessment. We look at threats, vulnerabilities, and the likelihood that specific threats could exploit vulnerabilities to cause mission impact.
And that risk assessment process then will feed information into the risk response step.

How do we respond to the risks that we've identified? Do we accept the risks or reject them out of hand? Do we transfer risk or share risk with other partners, for example, or do we go into some kind of a risk mitigation strategy where we apply additional safeguards and countermeasures or security controls to again reduce that risk.

And again, the last piece is monitoring risk over time to see if what we had today in the risk area is going to be consistent with tomorrow. And if there is an increased level of risk, we want to be able to respond to that over time.

Again, this is a moving train. The adversaries work 24-7, thinking up new ways to exploit vulnerabilities in our systems to cause that impact and we have to be a step ahead in order to make sure we're well protected.

Julia Allen: Excellent. So as you said earlier, this is an evolution. You start with where organizations and people are, and you take them through and educate them about this process. But for those who are just getting started, or are trying to move beyond just their tier three level activities, those about managing risk for specific information systems, what kind of advice do you offer or recommendations do you provide as a set of steps for getting started?

Ron Ross: Well I think, by far, the most important thing is to get the senior leadership involved within the organization and that may not always be the easiest thing to do. Most senior leaders today will readily admit that security is important, and it's a part of their risk management activities. But saying that and actually understanding what the risks are and how the enterprise is susceptible, based upon the kinds of things they're currently doing, is another matter altogether.

So getting senior leaders involved is really critical up front to get their commitment to reengineering the organization's processes to be more aligned with some of the things we're talking about in 800-39.

And that really may start with very simply, education and awareness training for the senior leaders, just bringing them up to speed on some of these concepts and how they relate to their business success. And I think that's the bottom line, always relating things to mission and business success because that's the reason why enterprises exist at the end of the day. Security and risk management are only tools to help us be successful in that space.

The second thing I would recommend is take a hard look at the core missions and business functions of the enterprise, and try to prioritize those, if they're not already prioritized.

And then the third step would be to look at the current commitment to enterprise architecture. Are they just giving it lip service, or is there a very serious enterprise architecture program to look at consolidation, standardization, and optimization? Again, the core concept in enterprise architecture are, try to manage complexity. We have very complex IT today and in order for us to be able to apply the right controls to the right place at the right time, we have to understand how all that technology fits together. And enterprise architecture is a very powerful tool to help us try to manage complexity.

And then integrating the security within the enterprise architecture so we don't have a separate architecture. We integrate those security features into the architectural decisions that we're making. I think if we can start with those three fundamental aspects, we will then be well on the road to of the long journey that will take quite a bit of time but you have to take that first big step.

Julia Allen: Well I won't be doing justice to the path that you've just laid out, but would it be fair to say that you need to put all of your thinking about security controls and security practices and tools and techniques at the system level, you need to work hard to put those in a meaningful context so you can be smarter about where you spend money. Is that would that be a fair way to net it out?

Ron Ross: Absolutely. Not only fair, but it's well-stated. And especially in a climate today where the threat space is getting more sophisticated, and our resources are fairly constrained, we have to work smarter. And I think the 800-39 three-tiered concept is a way of saying, "Let's work smarter.

Let's understand what's really important within the enterprise, understand the threat space, and then try to take appropriate actions all the way through investment decisions, all the way down to that last firewall on that last component. But thinking, every step of the way, is every action we're doing going to reduce our risk? And what should that risk level be, in order for us to really have a probability of mission success?"

Julia Allen: Right, because clearly you can't secure everything. You can't button down everything at your most desirable level of risk. So you have to make tradeoffs; you have to make decisions, and you have to accept that some things are going to be exposed, correct?

Ron Ross: Exactly right, exactly right.

Julia Allen: Great. So Jim, as we come to our close, I'd like to give you one more shot at the air space. Are there some other closing points that you'd like to highlight?

Jim Cebula: Yes, I think all of this is very timely. And like Ron mentioned in the response to the previous question, these issues of limited resources and having to do more with less. And in that light, we're starting to see a lot of focus, particularly in the federal government, on cloud computing. And we have a report coming out of the Federal CIO's office that, correctly I think, presents some pretty compelling business and financial benefits to transitioning services into a cloud environment to the extent that agencies are being encouraged to think cloud first in the deployment of enterprise services.

But at the same time, there's a lot of good work going on to develop, both on the commercial side and in the government side, technical measures that organizations should be thinking about to address new risks that might arise due to implementation of cloud services.

And all that is very important, but it falls right in line with what we've been discussing today on the podcast that you really, if you want to consider managing risks, you need to have a sound process, starting with the three tiers that are described in 800-39 starting at the top.

So it's really just an extension of sound risk management practices the way we've been discussing them today. And I think you'll find pretty consistent treatment of that, certainly in the 800-39 document, and what you have in RMM. So as agencies are thinking about cloud computing, for example, a lot of the tier two activities that you see in 800-39 are things that you would really need to consider and there's some linkage back to the Resilience Management Model in the external dependencies (EXD) is one of the processes that we cover that somebody could look through to help work through those tier two activities.

Julia Allen: Great, great. Well, Ron, we've barely discussed the tip of the iceberg, so do you have some resources where you can point our listeners for further information?

Ron Ross: Absolutely. All of our pubs, standards, and guidelines can be found at the NIST website. There's a wealth of information out there that you can download free of charge, and PowerPoint presentations, and you can also--there's contact information there too. You can call us or send us email, and we'll be glad to be a resource to you if you want to have some guidance on how to either improve your program or get one started. So we're always there to help you guys improve your security programs and manage risk.

Julia Allen: Excellent, and, Jim, do you have some pointers for our listeners?

Jim Cebula: Yes, certainly the complete body of work to the CERT-RMM on the CERT website. We have a resilience page. I think the link will be in the show notes. We had some previous podcasts in that area as well, and I believe we also have some contact information out there. So folks that want to get a hold of us to perhaps explore this further.

Julia Allen: Great. Well, Ron, Jim and I cannot thank you enough for the work that you do for our profession and for our discipline and for making valuable time today to discuss this very important topic. So thank you so much.

Ron Ross: Well thank you, Julia and Jim, it was a pleasure being with you guys today, and we really appreciate the opportunity to talk about some of the work that we're currently engaged in. Thanks very much.

Julia Allen: You're welcome, and, Jim, thank you for being with us today, and putting Ron's and NIST's work in context with some of the things that we're doing at CERT. Thank you.

Jim Cebula: Thank you, Julia.