Benchmarking Organizational Incident Management Practices

Featuring Robin Ruefle and Mark Zajicek Interviewed by Brittany Manley

----

Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

Brittany Manley: Good afternoon. My name is Brittany Manley. I am a cybersecurity operations researcher at the SEI's CERT Division. My guests today are two of my fellow CERT researchers, Robin Ruefle and Mark Zajicek.

Today, we are going to talk about their work on incident management, specifically, a benchmark that they have developed to help organizations manage computer security incidents. Welcome, Robin and Mark.

Robin Ruefle: Thanks, Brittany.

Mark Zajicek: Thank you.

Brittany: Before we get started talking about incident management, why don't you tell us a little bit about yourselves, the work you do here at the SEI, and maybe a little bit about what you did prior to your arrival here?

Robin: Okay, well, Mark has a very interesting history here, so I am going to let him go first.

Mark: I started way back in the 1900s, in 1987, before there was a CERT Coordination Center. I just happened to be working at the Software Engineering Institute at the time when the Morris Worm hit, and the CERT Coordination Center was established here at the Software Engineering Institute. My boss was the director of the CERT Coordination Center, so I was able to help support some of CERT's activities during the early months.

Then, I was fortunate enough to join CERT's Incident Handling team in 1992 as the internet was growing, and the number of people coming to us for help and assistance was growing. During that time, we started reaching out and helping other people create their own computer security incident response teams [CSIRTs], and it hasn't stopped since.

Brittany: That's great, Mark. Robin?

Robin: An interesting thing about Mark and I working together is we have actually been doing this work together in CERT since 1998. It is a pretty long time to be on the same team. That doesn't happen very often. We are pretty proud of that. I came previously from the University of Pittsburgh, where I worked at the Computer Center for Faculty and Students. Before that I worked in the state government for Pennsylvania in the controller's operations in their new systems division. But it was very exciting to come to CERT, and I came here 21 years ago, so I have been here a long time. I was able to join in work that was already established that Mark and others in the team, Georgia Killcrece and Moira West Brown, were doing at that time as far as building CSIRT capacity.

We had the really exciting piece that we were able to do some of the first documents related to computer security incident response teams. We did the *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Well actually, some of the people I mentioned did the initial one, but then Mark and I were able to work on the updates. We did some of the first assessment instruments specifically for computer security incident response teams. We have continued that work since that time. I am now working in the capacity as the team lead for CSIRT Development and Training. We have expanded our work in to looking at security operations in general, and we also have expanded that work. We work side-by-side with the National Insider Threat Center here at CERT.

Brittany: That is great. That is a great background. Let's turn our attention to incident management. Before we talk about managing incidents, let's talk about the problem at the root of your work. So, speaking from experience, what problems do you see organizations experiencing when trying to adequately respond to those security incidents?

Robin: I would say we have seen a lot of similar problems over the years. You would think as things grow that the same problems would go away, but what we see is the same type of problems I think come up again and again. So, maybe we will talk a little bit about that. To begin with, I think the easiest one is that a lot of people don't understand what incident management is, and they don't have a plan. They don't know where to start. They don't have a plan in place.

We like to say that incident response, incident management doesn't start when something happens bad to you. There is a lot of preparation work that you have to have done. There is a lot of team-building. There is a lot of team-testing that you have to do. People, I think, don't realize the amount of preparation that is involved. In fact, with some of the courses we teach, I think we usually have people walk out of them saying, *Wow, I didn't realize how many things are involved*. I think that is one of the big ones. I have a list of some others, but I will see what Mark thinks.

Mark: I agree with Robin. It is a lot about the different processes as we define them as part of the incident management lifecycle. Initially, from discovering that you have had an incident in the first place—whether or not it is through detecting signs of suspicious or malicious activity or receiving a report from someone else who has discovered it first—through the analysis part of it, and figuring out what is this that we are looking at—and then going through the whole series of possible response options that is appropriate to that particular activity. But as Robin mentioned, yes, it happens before the initial discovery or detection. There is a lot of preparation steps in place. Depending on what your role is within the organization, you may be involved in some of the actual activities to help protect and prevent an incident from occurring in the first place or maybe rely on other people who have that job, that role and responsibility.

Robin: That is actually a really good point that Mark is bringing up about relying on others because this is a problem that we see over and over again, too, is that very often there is a siloed approach to incident management. Really, when we talk about it, incident management is part of a much broader risk management perspective. It is one piece of that risk management and how you manage the threats to your critical assets. That means that you can't work by yourself. That you have to, especially with incident management…We like to say everybody in an organization has a role in incident management, whether it is reporting something suspicious, or helping to collect data or information or evidence, or following those policies and procedures that are in place to help prevent bad things from occurring in your organization. Very often, we find that that communication and coordination is the key that is missing.

One of the stories we like to tell in our classes that we teach is that very often we do assessments of organizations. We are actually using a version of this document that we are going to talk about today. I remember the first couple of times we did it on our team. What we found when we wrote up our findings was that the majority of the real problems that were affecting the organizations we had just assessed were typical organizational issues: lack of communication, lack of notification to the right people were involved, not involving all the different people that may be a stakeholder, and then not coordinating the response. So, you would get duplicate effort. You would get people left out that were critical to ensuring that there was a robust response that happened.

I do remember that one of our colleagues at the time, David Mundie, was very upset that it was just the organizational issues. We were surprised. It wasn't the technology; it was the organizational issues. Being part of that large organization, having better communication and coordination is so important. We see that over and over again. We also see—I would say that people rely on—we almost call them heroes, the heroes. They are the people who are going to work five days in a row to resolve an incident without sleeping. But if that person leaves, what happens? So, you have to institutionalize your processes. You have to make sure that everybody knows what the process is. You have to keep it up to date with the changing environment. You can't rely on just one or two people because they become single points of failure. We watch that happen again and again.

We have had some organizations come back three times to our Creating a Computer Security Incident Response Team course. We want to say to them, *Why are you coming back again?* It is because they didn't institutionalize the processes. They relied on particular people, and as soon as those people left, the relationships they built, the knowledge that they had, also walked out the door. So those are some of the other problems we see. Is there anything that you would add, Mark?

Mark: You covered most of the key points, and again, a lot goes into being prepared. That's a key part of that. You don't want to wait until something happens and then figure out, *Now what do we do*? Part of our [incident management] capabilities and our assessment process is looking at some of those preparatory steps to make it more formal and to identify roles, responsibilities, points of contact, how you are going to communicate with whom, when, how. All these are very important to being effective when the incident does occur.

Robin: Certainly, the one you hear talked a lot about is the lack of skilled staff. There is not enough people, and even the people who are interested may not have the right training. There is a lot of important training, and what we are seeing is a convergence of a lot of different disciplines that are supporting risk management and incident management. It is not just understanding operating systems and networks. It is also understanding processes, communications that we talked about. Now we are looking at artificial intelligence and machine learning, statistical analysis, all those things start to come into play. So it is a much more complex area, and you need a very rounded team. That, again, is why it is so important to be able to coordinate and reach out to other parts of the organization. It can be even people in your training department, your PR department, HR, human resources, rather. There are a lot of people that could be involved.

Brittany: Going along with the people and processes in preparation for incident management, you recently published a technical report in which you outlined various capabilities related to these incident management activities. This report also includes a benchmark to help organizations manage computer incidents that can threaten their security. Tell us a little bit about that benchmark and how organizations can use this to their advantage.

Robin: Let me give a little broad overview, and then I would like to ask Mark to talk a little bit about the history of the document, because it has a very interesting history. Our *Incident Management Capability Assessment* is actually a workbook assessment that you can use to do a self-evaluation. Or you can have a third party come in and use the instrument to do an assessment of a set of what we call incident management capabilities. Really, it extends beyond that and hits some of the other areas of cybersecurity operations. It also takes a look at how those things need to be institutionalized.

When we take a look at that broader set of capabilities, what we're looking at is good practices for preventing, detecting, and responding to threats, risks, attacks against your critical assets and against your organization, your constituents. What we mean by constituents, these are the people, the stakeholders, that a computer security incident response team or security operations center or a risk management team are serving. They're the ones that they're helping. Mark can tell you a little bit about the background.

Mark: We got started in this work about 2000, 2001 when we were working with the United States Department of Defense, who had issued some directives for all their services that had to provide, what they were called at that time, the term was computer network defense. Everyone had to either be a computer network defense service provider or get their information technology networks from an authorized CNDSP, computer network defense service provider. These providers had to be certified and accredited, and as follow up to these directives that were created, we worked with a number of other organizations to help the Department of Defense come up with what was called *Evaluator's Scoring Metrics* for the certification and accreditation of these computer network defense service providers.

At that time, computer network defense was defined as the protection, detection, and response to incidents in these types of activities. So those were the three primary categories that we looked at. We looked at specific activities and best practices to make sure that the organizations were doing these things and they had another category for sustaining those primary core protection, detection, and response categories. So, we worked with them to come up with their own version, and later on, we worked with some of our federal civilian agency partners to come up with a non-DoD version, and have modified it several times since then.

We published a generic version back around 2007, and this recent report that came out last year is an updated version of the capabilities that go across those categories, as well as we added a new category for the preparation, preparing multiple capabilities to be able to provide the Protect, Detect, Response functions.

Robin: We have a lot of appreciation for the Department of Homeland Security who we were able to work with to actually build the federal version. Those were called the F-CND, so the

Federal Computer Network Defense Metrics. The old version that we did, a generic version, that means we could publish it, we could put it out on our website, and anyone could download it and use it. That public, generic version, we called metrics, and it had a list of things that weren't grouped.

One of the things with this new update, as Mark said, we added the preparation part. We added a lot more guidance and a lot more information on the capabilities and what you're looking at. Basically, you are looking for, *Do you have the right policies, procedures, controls, staff in place and institutionalized? Do you have all the components to do incident management and some of the corresponding, related activities like vulnerability management, malware analysis, insider threat?* So there're capabilities associated with each one of those. The nice thing about this workbook, this assessment instrument, is you can use it the way that fits you best.

You don't have to do it for all the sections. There're the five sections as Mark said, prepare, protect, detect, respond, and sustain. You might just want to focus on one. Like in the prepare, there's a whole section on program management, and it looks at some of the things that we've just mentioned. It says, *Do you have an incident response or incident management plan in place?* Then it lists a number of criteria, and it says, *And here's what we mean by this*. So, to meet that capability, you have to meet all the requirements that are—actually we have a category called required. You have to meet all of those. And then there's some on institutionalization.

Not only do you have a procedure written, but do people use it on a daily basis? Does everyone know about it? Can you easily access it? Is there a hard copy of an online copy? If we went and interviewed people in your staff, would they all tell us, *Yes, this is the policy and we all do it the same way*? Very often that's not the case, too. Also, with this document, or this assessment instrument, we have capabilities with priorities. Would you like to talk about the priorities?

Mark: The priorities again are somewhat based on how the Department of Defense's *Evaluator's Scoring Metrics* were designed. They had four levels of priorities with the idea being that as time went on, some of the lower priority items that you may not be doing weren't of top concern. You wanted to try to meet as many of the priority one capabilities first because they had a more serious impact. So to try to focus your efforts to try to be best across the whole range of different activities gave you some way, because oftentimes, it's difficult to address all of them.

In fact, many organizations, depending on the size and type of the organization, it is typically not the case that one individual or one group is performing all of these capabilities. They are split off across multiple different groups or subparts of the organization. That is also another reason why in performing these self-assessments or evaluations, oftentimes you may want to scope it to a small subset of all the different capabilities to start out with.

Robin: Sometimes there are capabilities that you don't do because of the type of organization you are. So there are options to leave those off, or say, *This is not applicable*. However, we do have a little bit of a red line where this is something that is a really key priority area that we think everyone should at least consider doing. The example I gave you when I said, *Do you have an incident management plan?* We wouldn't allow someone or we would not recommend that they leave that out because they didn't have one. No, they should go through and they should see what they have and what they don't. That is also what we find with using this assessment instrument. It can really help you see where you are and where you need to go. It can help you define your current state and then help you identify, *Here are the things I am not doing that I would like to do, and can I create my to-be statement*? *Can I prioritize how I can get there*? So not only does this workbook allow you to kind of evaluate yourself, but you can use it to plan for your process improvement, and that is where this came from.

We worked with some people, Chris Alberts and Audrey Dorofee, who were from the risk program at the time at the SEI, to help us create this instrument. It really comes from a lot of the process improvement work within the Software Engineering Institute. Also, you can take a piece of it, and you can look at, for example I will use the incident management plan again. If you go through and it says, *Do you have these things*? Well, you don't have to use this document to evaluate yourself. You can also use it if you are planning your team. It doesn't have to be a computer security incident response team. It also applies to security operations or SOCs. It can apply to any type of security-type team.

What we like to say, if you are detecting, analyzing, and responding to computer security incidents or information technology incidents, read this document because it is applicable to you.

We don't like to get too tied up in actual names of things. We look at, *If you are doing these functions, this is important to you. You are our audience.*

Brittany: One of the areas that we like to focus on in this podcast is transitioning our work and ideas to the stakeholders and the public. If I am responsible for incident management in my organization, where do I start? You mentioned using these as a self-assessment, but where do you start? What are the resources that you could use to begin to think about a lot of these processes and incident management activities?

Robin: I like to go back to something I mentioned about incident management being part of the whole risk management process. If we start at the high level, one of the things we say too is that you have to think of this in the context of your own organization, what the organization's mission is, and you have to understand that. You have to understand what the business objectives are.

You have to understand the key critical assets that keep that business functioning, because what you are going to be looking at is, *How do I protect these actual assets? How do I detect when something is malicious, trying to attack or damage those assets?* And then, *How do I actually respond?* Depending on the type of assets, the type of organization, those things can be different. You do have a path of things, the incident handling lifecycle like Mark mentioned, but there is going to be unique areas because of the organization you are. Very often people in incident management, we found, would only look at the technology side and not understand that you have to look at technology in light of the business, the business missions. It's all tied together. This helps you identify some people to pull in from risk management, from your executive levels, to help understand and to help build your plan. So, that is like on a very high level. Sometimes people say, *Well, maybe that's a little bit too down in the weeds for me. Where do I really get started?* The nice thing is, is that there is a pretty big community out there of people in the security operations and computer security incident response team arena. There is a lot of information out there, a lot of things that can help guide you.

Some of the things to take a look at are some of the NIST documents, the National Institute of Standards and Technology. There is a document that they have produced, and I think the latest update was in 2018. That is the Cybersecurity Framework. The Cybersecurity Framework takes that whole part of cybersecurity. It almost sounds a little bit like how our document is broken up, because it looks at, *How do you identify what you have to protect?* It is looking at asset management and inventory, access control, things like that. It has a protect section. It has a detect section, a response section, and a recovery or recover section. It has a lot of the sub-functions of the services that are under these areas. That can give you a broader perspective and see where incident management fits in and understand the types of activities that you might have to actually perform.

NIST also has another guide, the *Computer Security Incident Handling Guide*. That is 800-61 Revision 2. You can look at that, and that gives you a broad picture.

There is NIST documents. There is documents that we at CERT have produced. I mentioned the *Handbook for Computer Security Incident Response Teams*. There is work that the Forum of Incident Response and Security Teams [FIRST] is doing to define a services framework and calling out security event management, incident management, situational awareness, and any ties to cyber threat intelligence, vulnerability management, and knowledge transfer, which is actually looking at the training, education, policy advisement. There are a lot of different areas out there, a lot of documents and resources. There are various trainings.

We provide training. We have courses for computer security incident response teams, security operations centers, but we also have risk management-type courses too. There is a large body of work in the CERT Resilience Management Model, CERT-RMM, that also gives you that high-level approach.

There are a lot of different things out there. If you are going to start anywhere, I might say start with the Cybersecurity Framework, but also look at some of the documents that we have at CERT because we delve down into it a little bit more.

Then there are certainly classes that you can take across multiple different training providers that can help too. Those are some of the things I think of. Is there anything that you would add, Mark?

Mark: In addition to what Robin mentioned, there are many other organizations that have resources that are available online. In addition to the National Institute of Standards and Technology and the various resources and publications they have, FIRST, the Forum of Incident Response and Security Teams on their website, first.org, has a lot of free information. You don't necessarily have to be a member, but it is available to you. There are other organizations around the world. FIRST is an international organization, but in the European Union, there is an agency for network and information security called ENISA, E-N-I-S-A. They published a lot of resources available, again, free on their website. Of course, going back to our own *Incident Management Capability Assessment* report, if you look at the appendix, the appendix has a list of all the different capabilities organized by the higher-level categories and sub-categories. You could use this as a simple checklist if you are trying to identify which things you may want to build or include if you are just planning on getting started. If you don't have an established response team already, you can use this as an intermediate checklist to get you started.

Robin: Actually, thank you, Mark, because I apologize. I misspoke. It's the National Institute of Standards and Technology, and I said Science and Technology, which is always what goes in my head for some reason. I wanted to make sure that I corrected that.

Brittany: Thank you for those resources. I think that is very helpful. Now you had mentioned and obviously in your experience over the years, this body of work has grown and developed based on best practices and how threats have evolved over time. So, where do you see this body of work going in the future based on your expertise and experience in the field?

Robin: Thanks, that is a great question. It is interesting because, as we said, so many organizations are unique and have unique needs. What we would like to see, and what would like to do in the future is maybe do some customization.

One of the areas, if we go back to one of your first questions about problems we see, small- and medium-size organizations very often don't have the resources. They might not have access to some of the materials to be able to build their incident response plan and management. We would like to see, *Is there something that can be developed for small- and medium-size organizations to help them?* There are resources to help understand incident management, but we don't have anything to just go in and assess them and help them with process improvement. So, we'd certainly like to look in that area.

Along with that, there are other types of teams. National computer security incident response teams that are responsible for a nation-state or an economy, and act as a coordination center within their country to get information about incidents to the right people within the country, the stakeholders, and also to share that information with others in their region or possibly globally through FIRST. They have some different activities. They focus a lot more on the coordination, whereas an organization like a manufacturing company that might have an incident management plan is really looking inside their own organization and how to detect and handle and respond to incidents. We'd like to a little bit more customization.

FIRST, we mentioned, is in the process of releasing an updated *CSIRT Services Framework*. One of the things we'd like to do there is maybe redo the version of the *Incident Management Capability Assessment* to actually match the new services list. The information's not going to change, because all the information is still relevant. It just might be organized in a different way so that you can find things in a fashion similar to *CSIRT Services*. At least those are some of the things that are my long-term agenda.

Mark: That is something we have seen too, just as this field grows and evolves, just a change in the terminology: what we called something 20 years ago, we might have a new term, new jargon for it today. So just bringing it more current into today's world. That's some of the problems that we have to deal with.

Brittany: Great. Well, Robin and Mark, thank you for joining us today and thanks for this discussion. If you would like to learn more about Robin and Mark's work in this field, please go to resources.sei.cmu.edu. You can click on the Browse by Author tab and look under R for Ruefle, R-u-e-f-l-e, or Z for Zajicek, Z-a-j-i-c-e-k.

We will include links to resources mentioned during this podcast and in our transcript. Thank you all for joining us today.

Robin: Thank you so much, Brittany. It was a pleasure to be here with you and get to talk with my colleague, Mark, about these important issues. I just do want to say one last wrap-up piece. That is, if we go back to the question you ask about, *What can I do?* The thing to do to start anywhere is to say, *If something happens, what are my steps going to be*?

To think about that in advance. Even if you are a small organization, *Who am I going to call? Do I have a contract?* Have that at least discussed ahead of time. Even if it's a small plan with two or three steps, just get that down, and then you can expand on it as your organization grows.

Brittany: OK, that makes sense. Preparation is key.

Robin: You got it.

Brittany: Thank you, Robin. Thank you, Mark.

Mark: Thank you.

Robin: Thank you.

Thanks for joining us. This episode is available where you download podcasts including SoundCloud, Stitcher, TuneIn radio, Google podcasts, and Apple Podcasts. It is also available on the SEI website at sei.cmu.edu/podcasts and the SEI's YouTube channel. This copyrighted work is made available through the Software Engineering Institute, a federally funded research and development center sponsored by the U.S. Department of Defense. For more information about the SEI and this work, please visit www.sei.cmu.edu.

As always, if you have any questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you.