Conducting Cyber Exercises at the National Level
Transcript

Part 1: Objective, Motivation, and Getting Everyone on the Same Page

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT, working on operational resilience and software assurance.

Today I'm pleased to welcome Brett Lambo. Brett is the Director of the Cyber Exercise Program with the U.S. Department of Homeland Security's National Cyber Security Division. I'd also like to welcome one of my colleagues, Matt Butkovic, a member of CERT's Resilience Enterprise Management team.

Today Brett, Matt, and I will be discussing something I think is pretty interesting: how scenario-based exercises can be used to help organizations identify and mitigate their cyber and IT infrastructure risks. Exercises can be conducted at the state, regional, federal, and international levels. And our listeners might be familiar with Cyber Storm. It is one example of a national-level exercise that we'll be talking about towards the end of the podcast. So with no further ado, glad to have you with us today, Brett. Thanks for joining us.

Brett Lambo: Oh, pleasure to be here. Thank you.

Julia Allen: And Matt, great to have you on the call.

Matt Butkovic: Great to be here.

Julia Allen: Okay so Brett, we're going to be talking mostly about your program today, which is a great opportunity for us here at CERT. So could you, just by way of an introduction, could you tell our listeners a little bit about the primary purpose for cyber exercises, and from your point of view, why you found them to be effective.

Brett Lambo: Sure, yes. The real value of conducting cyber exercises -- very much like with normal, traditional exercises that people might be used to seeing on the news where you've got fire trucks in the parking lot and people with ketchup on their foreheads and things like that -- the real value of that, especially in the cyber arena, is to be able to really create a no-fault environment for people to road-test plans and procedures that they have in place for cyber security matters, cyber incident response.

Or actually, most importantly, plans and procedures that they think they have in place. A lot of times we'll write standard operating procedures and get together with the people that we think we coordinate with in incident management and incident handling.

And we'll think we're all squared away until something happens and we realize that maybe our coordination paths weren't as well developed as we thought they were. So what an exercise allows you to do is come up with a fictional scenario and a fictional adversary and a fictional attack and really have some fun in exposing everybody to this event. And to step through what

you think your procedures are in a way that allows you to expose where there might be gaps, where maybe you have some redundancy in capability. And, more importantly -- and it's a little bit of the squishier part is -- you really get to know the people that you're interacting with, or you're supposed to be interacting with.

One of the biggest values we've found in conducting cyber exercises is, as this community continues to mature and as the relationships are newly developing and flourishing, we can establish those relationships. So you know who's supposed to be on the other end of the phone or you know who your customers are or you know who your support is in the event of a major cyber event. And you're able to see who's got what role and responsibility in that.

So, like I said, first and foremost they should be fun. But really it's a great way to walk through some procedures and lay yourself bare a little bit without, absent the risk that you're actually going to do your organization or your networks any harm.

Julia Allen: Excellent, excellent. So when you're putting these exercises together, clearly there are lots of key players. Could you tell us a little bit about some of the critical roles? I'm sure it depends on the exercise -- but the typical participants and stakeholders that are engaged in a cyber exercise?

Brett Lambo: Sure, absolutely. We're all fond of saying that the things that we are involved in are a little bit different and a little bit unique and it's usually because they are. And that's especially true in cyber security. We throw the word "cyber" around a lot, but the composition of the community, that stakeholder community, really is pretty unique.

Nowhere is it more true than in cyber security that the private sector owners and operators of the infrastructure are really the prime -- they're really analogous to the primary first-responders. They're the ones with direct access to the networks and they have the best idea what information is flowing across those networks.

So you've obviously got to have the owners and operators of the networks and the equipment and antivirus software vendors, things like that. But obviously government's got a big role to play as far as coordination is concerned. So the cyber infrastructure is really a foundational element of the larger critical infrastructure. The National Infrastructure Protection Plan outlines those 18 critical infrastructure sectors. But the important thing is you've got to get all those people whose critical functions really depend on the operation of the Internet or the reliability, the security, or the resiliency of the infrastructure to conduct their day-to-day business.

But basically at the core of it you've got your net defenders and you've got people that are involved in the day-to-day monitoring what's going on out there in cyberspace -- patching, hardening networks, patching systems, and making sure that security risks are mitigated. So you've got those people who are the operators. But then as you increase the scale and complexity of the exercise, you start to bring in policymakers, you start to bring in public affairs officials, obviously emergency managers. Cyber events can have physical implications that would necessitate some sort of a traditional first response.

So a lot of it is based on the objectives you're trying to get out of the exercise. You look at, "Here's where we're going to set the boundaries of the game space and here's what we're going to do. Here are the objectives we'd like to get at. Now let's get together the people from industry, academia, government, law enforcement, intelligence all of those people that might have capabilities to bring to bear." You bring those people and really start to test out the relationships they have with each other.

Julia Allen: As I listen to you describe this, I mean I'm sure it depends a great deal on the exercise itself and if it's regional or if it's national we'll talk about that in a moment. But how do you get all these folks on the same page? That seems to me it would be a huge challenge, of course depending on scale. But how do you get everybody headed in the same direction?

Brett Lambo: Well, you threaten them. No, you ask nicely. The people that we get have really come voluntarily, understanding the magnitude of what's at work here. And more importantly, it's a case where some of the participants you can get to come by making the case that you don't know what you don't know yet. And that includes people who have spent a lifetime behind a keyboard coding (and they think that they're the cyber security experts) who might not necessarily then see what are the broader implications at a policy level or a national security level.

So basically what you do is make the case that, "Look, we're all in this together. And really, we always possess" -- and when I say "we all," at that stakeholder community -- "we all possess unique capabilities that we need to be complementary of each other's capabilities." So here at DHS we've got one set of capabilities, and the law enforcement community's got another, and the private sector's got another, and academia's got another, and research and things like that.

None of those is sufficient to adequately mount a good defense to a major cyber event. So it very quickly becomes clear to people that we need each other. And just as I need someone else to be involved in this exercise, boy, I got to really bring my own capabilities because they might need something I have. So there's a lot of cajoling and a lot of meeting and a lot of outreach but it quickly becomes clear. We've never struggled from lack of interest. I'll say that.

Julia Allen: Obviously the mission is the unifying theme. Everybody can identify with the mission and what they're trying to learn and what they're trying to prepare for. So I think that in and of itself is probably fairly compelling.

Brett Lambo: Yes, absolutely

Part 2: Discussion- and Operations-Based Exercise

Julia Allen: So in some of your literature -- in particular you have a Homeland Security Exercise and Evaluation program overview available on your website -- you do talk about a range of exercises in a couple of different categories. I think it might be helpful to tell folks a little bit about these or maybe pick out a few of your favorites.

Brett Lambo: Sure. It's basically a project management, program management methodology for planning and executing an exercise. But basically there's two type of exercises. You can have discussion-based exercises and operations-based exercises. And so as they go from left to right on a graph, they start to get bigger in scale and bigger in magnitude but it doesn't necessarily mean that one must come before the other. Again -- and you brought it up, Julia, exactly right -- it depends on the objectives you're trying to get at.

But discussion-based exercises are really something you can do without a lot of lead time and a lot of planning. And it's really a good opportunity; there's a few different types. You can do a seminar or a workshop or a table, what's called a tabletop exercise (which is really the most common discussion-based exercise), and a game. The real difference between those is you would use a seminar basically as an educational forum. We joke that it's like a chemistry lab where the first half of the day you can teach people what they need to know and the second

half of the day maybe you do a tabletop exercise that's akin to the lab, where you light things on fire based on what you learned in the morning.

You can have a workshop. And one of the big benefits of an exercise is you can use it as a forcing function to create procedures or create relationships where they don't already exist. And that's one of the benefits of a workshop is that you can get everyone together and say, "Look, we know we have holes. It wouldn't really do us much good to step through a scenario. Let's start to figure out where we need to develop some procedures and get at doing that." I mentioned a tabletop. A tabletop is probably the most common or at least the most common in public perception. Tabletop is where you really -- you get everybody around a table, or a series of tables, and you can present a fictional scenario, or a simulated scenario. And you really get people trying to validate the procedures that they think they have in place or the procedures that they do have in place.

So it's a really useful environment for saying, "Okay, in the world as we perceive it now, if this happened, how would we respond to it?" And a game is a little tweak on that, where you can have fun in a game by saying, "Well, let's see what happens if we were to do X, even if it's not what you have in your articulated plan." So, again, discussion-based exercises are an incredibly efficient tool for being able to get some people around a room and just stimulate discussion.

Now operations-based exercises -- drills, functional exercises, full-scale exercises -- again, that's really your chance to then go and stretch your legs a little bit. That's where you can say, "Okay, well, we've got these procedures and we've got these objectives. Now let's actually sit at the workstations we sit at." And in a cyber exercise, that's one of the things that makes it unique. Rather than pulling the fire truck out of the station and turning the sirens on, you might actually just have somebody in an operations center doing that kind of thing virtually. So with these operations-based exercises, you really want to have the people that are responsible for responding, getting real-time information, doing real-time information sharing, getting things as if they would be getting them in real world, and then watching the response and watching how they're actually going through what they're supposed to do.

And a full-scale exercise is just that next step, where you're basically -- you're doing the response actions and then you're actually deploying resources as you would if it were a real-world event. Again, like I said, it's any mix of resources or magnitude that you think will fit your needs. You can find the kind of exercise, be it a discussion- based or an operations-based exercise, that'll hopefully get you there.

Julia Allen: Great. Well, do you find that there's some variation in the type of exercise that's most useful if you're working at a regional level, local or a state level, or a federal level? Or does that really not affect -- we talked about the objectives. Is it more the objectives than the scope of the exercise? Is there any particular variation on a theme there?

Brett Lambo: Yes. I mean, you're right. It really is more about the objectives than the type of the exercise. And again, just being blunt, it's about the maturity of an organization or of a community. You wouldn't want to build a full-scale exercise around an organization or a community of people that might not have very well-developed operational plans or operating procedures or things like that.

So really a lot of times, if your initial objective is to create the burning platform for continued collaboration and actually just setting a watermark for where you are at a point in time, then that would steer you in the direction of a smaller-scale, discussion-based exercise where

you're not actually exposing the fact that you don't have a process in place if you already knew that you didn't. And that's true in regional settings and in state and local settings and individual organization settings.

What we're trying to do now as a community is really build capacity. And again, there's no denying that this is an important topic but a lot of times you have to reinforce that because, especially with cyber, senior leadership doesn't always see things on fire and so the magnitude of the risks and the vulnerabilities aren't always clear. So it helps you if you can have those smaller-scale discussion exercises, you can create that platform and say, "Look, this is a big deal."

Part 3: Cyber Storm: A Full-Scale National Exercise

Julia Allen: Excellent, excellent. Well, let's turn to a case in point, which is Cyber Storm. And I know you've conducted several rounds of that particular mission objective or exercise. So it is an example of a full-scale exercise. Many of our listeners may not be familiar with it, so could you tell us a little bit about the Cyber Storm series. And to the extent you're able to share, perhaps some of your key lessons learned so far.

Brett Lambo: Sure, yes. We've done three Cyber Storms -- and I always say that two's a coincidence and three is a series. So now we can actually call it a series. The most recent one was at the end of September of 2010.

Really Cyber Storm is intended as a large-scale, national-level cyber exercise. And I say national as opposed to federal because it is truly that. The private sector is deeply involved in not only building the scenario to make sure that it's credible and to make sure the scenario actually reflects what's going on out there on the wire every day, but also that it is technically sophisticated enough to really challenge even the people with the most amount of capability.

The real goal of the exercise is to look at how well we as a nation can navigate the response to a significant cyber event or series of significant cyber events. And this most recent version of the exercise -- we were lucky to have a draft version of what's called the National Cyber Incident Response Plan in place that we were exercising. That cyber incident response plan was absolutely critical to the exercise because it gave us the basis for what we were going to look at. How do we as a nation step through an incident? What are the roles and responsibilities? Where are the lanes in the road? So who has the authority to do what to whom and when and where and ask for what and all of those things.

So when something's happening and the private sector is managing the incident on their wires but the government has a responsibility for situational awareness and coordination and we've got international partners involved, what we really try to do is use Cyber Storm as a big event to really look at how mature and how well developed our procedures and our plans are.

And it's fair to say that as the series has evolved from one to two to three -- we've done them every two years -- what's interesting is people always ask, people want to know, "Well, did you fix it? Did you fix what you learned?" Well, really, the exercise offers you a window into time and to what your capabilities are at that point in time. And if you really look at the evolution of our national capabilities since 2006 to 2008 to 2010, it's a very steep curve. And the amount of capability that we have a nation now to defend against and mitigate the effects of a cyber incident, those have just multiplied by orders of magnitude over time.

The exercise is always going to expose how important certain things are: the need to share information, the need to work collaboratively, the need to inter- governmental and public/private coordination effectively. And so what we learned is, over time, we're making a lot of progress in building the structures and putting the plans in place and establishing the relationships to do that. And the devil is in how. And that's the real value of the Cyber Storm exercises, where we keep digging deeper into: Is how we do what we say we do, is that directionally and conceptually sound? And are there places where we can change some things or course-correct, and make improvements there? And that's really -- our after-action report for Cyber Storm III will come out sometime this year, early this year, and when it does we'll be able to talk a lot more about specific findings. As a summary, it's safe to say, we got a lot of learnings on things we need to do better specifically in how we do the things you need to do to respond to an event.

Julia Allen: So are you planning that -- as you mentioned, three makes a series -- is there going to be a Cyber Storm IV as far as you know? Or is that still up for discussion?

Brett Lambo: It's still up for discussion exactly what those activities will look like. We've obviously got -- FEMA's got the National Exercise Division and the top-level, national-level exercise series. And we've got all kinds of activities that we can engage in under the Cyber Storm badge.

And so there will definitely be continued activities that are following in the footsteps of the first three Cyber Storms. And we will be -- it'll all be circular related to that Cyber Storm exercise. But whether that means that it's going to look like one big Cyber Storm IV, like Cyber Storm III was, that's in development. And we just want to make sure we're using, making best use of everyone's time and resources. Because it does take time and resources to do these and we want to make sure that we're not being duplicative of other efforts and that we're able to leverage off of other things that are at work.

Julia Allen: Excellent. So Matt, you've been very kind to let Brett and I monopolize the airspace. So as we come to our close, could you say a little bit about CERT's role in particular in working with the DHS Cyber Exercise Program and with Brett's staff?

Matt Butkovic: Sure. Absolutely, Julia. So we're assisting DHS in enhancing the state of the practice for cyber exercise in a few ways. We provide direct assistance in development of cyber scenarios.

In the case of Cyber Storm, we provide assistance in ensuring a high level of operational realism. We're also developing tools that help improve and foster repeatability of cyber exercise. We're designing processes and methods to define your objectives of the cyber exercise, to build credible and realistic scenarios, and then equip the cyber exercise owner with the tools to successfully execute that cyber exercise, and then translate those learnings into a series of steps that improve their capabilities to identify and respond to cyber incidents.

We've codified these learnings and the good practices in the industry in a document we've entitled "Enhanced Methods for Cyber Exercise." And we continue to develop scenarios and the input to scenarios for the cyber exercise program.

Julia Allen: Excellent. So Brett, first as we close from your point of view, do you have some resources, websites or other places that you could point our listeners for further details?

Brett Lambo: Yes. The DHS National Cyber Security Division website -- if you root around there a little bit, you'll be able to really get some insight into a lot of the resources that go into not only a cyber exercise. An exercise is only as good as the operational capability it's exercising. So you can read about the National Cybersecurity and Communications Integration Center (the NCCIC), US CERT, National Communications System -- all of those key players that are involved. If you look off the Cybersecurity and Communications, and specifically the National Cyber Security Division, you'll be able to get a sense for what we're actually exercising.

Julia Allen: And will there be -- you had mentioned the after-report for Cyber Storm III. Will there be a version of that that's available in the public domain?

Brett Lambo: Yes, absolutely. We are in the process of adjudicating comments and it's -- again, the exercise is a big community of people from a lot of different backgrounds and we cycle the report through them to make sure that it's right-headed and directionally correct. So we're working that out and there will be a report that's publically available. I'm reluctant to give an exact date right now, but we're pushing it very hard. It is priority number one.

Julia Allen: Excellent. And Matt, places you'd like to point our listeners?

Matt Butkovic: Sure. Listeners can certainly visit the CERT website and find a wealth of information about not only cyber exercise and measuring your organization's operational capabilities, but also a wealth of knowledge, a body of knowledge, regarding incident management and incident response.

Julia Allen: Excellent. Well, Brett, I can't thank you enough, now at the beginning of this new year, for making the time to getting us off on a good track and describing the benefits of this program that I think will be of great interest to our listeners. So thank you very much.

Brett Lambo: No, and thank you. It's been a pleasure to be here and I appreciate all that you do.

Julia Allen: And Matt, thank you for being on the call with us today. Sure do appreciate it.

Matt Butkovic: Thank you Julia, thank you Brett.