Developing a Global Network of Computer Security Incident Response Teams (CSIRTs)

Featuring Tracy Bills and James Lord as Interviewed by Suzanne Miller

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.

Suzanne Miller: Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. My name is Suzanne Miller. I am a principal researcher in the SEI's Software Solutions Division. Joining me today are Tracy Bills, senior cybersecurity operations researcher and team lead, and James Lord, security operations technical manager, both with the SEI's CERT Division. Today, we are here to talk about their team's work with countries throughout the globe in developing cybersecurity incident response teams, which are also called CSIRTs. I want to welcome both of you.

James: Thank you.

Tracy: Thank you.

Suzanne: Both of you are new to our podcast series, so let's begin by having you tell our audience a little bit about yourselves and what brought each of you to the SEI and the work that you do here, and especially what the coolest thing about your job is. Everybody wants to know that. Tracy, why don't I start with you?

Tracy: Sure. I have been at the SEI for a total of 10 years. I did have a gap in there where I left for a few months and decided to come back because I really missed the work. Before that, I worked at the Multi-State Information Sharing and Analysis Center, and before that, leading cyber threat intelligence teams for the Department of Defense [DoD]. One of the things that brought me to the SEI was the initial projects that I worked on involved helping the public and private sectors establish programs for sharing cyber threat information. Building those relationships and communities was a big draw for me, and it is also applicable in our current work where we assist teams around the world, developing their national incident response capabilities and their security operations centers and their national computer security incident response teams, or CSIRTs. One of the biggest things that I enjoy about this work is really the people, getting to meet and work with so many different people around the globe, all who are striving to improve the security posture of their organization in their country, which contributes to the cybersecurity posture of everyone that is connected to the Internet.

Suzanne: That includes us.

Tracy: Yes.

Suzanne: James, tell us a little bit about yourself and what is cool about your job.

James: Yes. I was at, it is called the Supreme Headquarters Allied Powers Europe.

Suzanne: SHAPE.

James: SHAPE. It is in Mons, Belgium. We used to like to tell ourselves that we were the stepchild of NATO because, you know, up there in Brussels, they are very glamorous, and SHAPE is not necessarily glamorous, but I was updating my alumni profile and I was contacted by the Software Engineering Institute because they were interested in going into international work, specifically incident response, with the global community. And that is what

brought me to the SEI. I think they told me nine years ago this month. I thought it was eight. It is actually recruiting people that will do the work because everything that Tracy talked about requires people that actually have the skill sets and then the initiative to do the work, because I think the work is very challenging, very demanding, and that is what I appreciate, is that we find folks that will do the work.

Suzanne: All right. I am going to do one quick aside here. I was actually at NATO in Brussels. My dad was stationed in Brussels in 1974 and '75, and I actually went down to SHAPE when I was in high school to do a speech and drama competition. I know exactly where you were. Anyway, that was years ago. James and Tracy, we are here to talk about your work with other countries in developing computer security incident response teams, the CSIRTs. And explain for us first what is a CSIRT, and how does it work?

Tracy: Sure. We like to describe it as something similar to the fire department. The fire department has a proactive role in educating people on how to prevent and how to detect a fire, what to do when one initially happens, and the fire department is the one who identifies what caused it, mitigates the fire, and then looks for ways to prevent it from happening again in the future. A national CSIRT, well, any CSIRT is similar. Their job is to establish services for their organization or whatever stakeholders they are assigned to as part of their mission. Their services may include anything from monitoring networks in order to detect cybersecurity incidents. Once those are detected, identifying how to respond to them, how to mitigate them, and prevent them from happening again. When it comes to national CSIRTs, they are unique in that they are responsible for a nation or economy, whereas other CSIRTs might just be responsible for their organization or company, or if they are a product CERT, they might be responsible for the products that the company develops in ensuring that they can respond to incidents that involve their devices. For the national CSIRTs, because they are, you know, protecting a nation or economy, they are responsible for coordinating the response actions for significant incidents that impact multiple entities across their nation or economy. They have a pretty large responsibility when it comes to cybersecurity incidents.

Suzanne: One of the things that I think might be different from a fire department is, you know, fire, I mean, there are different accelerants and things, but on the whole, I would say fire is a technology that is pretty well understood. Once you understand how fires start and things like that, you probably do not need to do constant refreshing on what is the latest and greatest thing. But with security, that is a whole different posture. We are

always inundated with new threats. There is another piece that I would assert that a CSIRT has to be aware of, is not just doing all the things to mitigate, but just keeping aware of what is happening in the world because the threat posture is going to be changing depending on where you are and sometimes what time of year it is. Is that something that is a big challenge for you, for helping people to understand what is involved in a CSIRT?

Tracy: Yes, and it is a big resource challenge for the CSIRT itself. Having the right staff that can be able to learn about new technology as it, you know, joins their environment or their stakeholders' environment and being aware of any of the new vulnerabilities for all of that new technology. It is kind of a constant cycle of new technology, new vulnerabilities, vulnerabilities in the existing technology you already had. It is definitely an ongoing learning process for the staff.

Suzanne: It is probably one of the things that I would think would be most exciting, but also a little bit daunting if I was going to be going into that. But let's talk about the other piece of this that has got a lot of variety associated with it, is the approach to setting up CSIRTs in different countries, right? Because, you know, a CSIRT in Belgium and a CSIRT in Brazil are probably not going to be the same, even though both countries start with "B." How do you approach things differently in developing countries, you know, technologically mature countries? How does that play out when you're working with these different entities?

James: The history of our work began in sub-Saharan Africa, specifically in Ghana. And then we eventually also moved to Côte d'Ivoire, both in Western Africa. Both would be considered emerging economies and both would be considered national CSIRTs that had resource limitations. They would not be in the same category as a Brazil or a Belgium. However, to Tracy's point, this type of these skills, this capability, this national CSIRT is a value to any economy and to any nation-state, Ghana not being different. The difference that I think we apply to this work is we do have a process. It is called the mentoring framework. We wrote that for the State Department and it was accepted by the State Department. And the mentoring framework, in a very simplistic way, is an x- and a y-axis, which is wants and needs. Our team focuses on the needs, not the wants. In line with that, we are not immune to what a country aspires to. We just try to focus on those elemental or baseline skills and services that will make you a success. In the incident response community, there are many who say, *You have to do incident response*. I always say that, *Yes, eventually you have to do incident response*. But if you want to demonstrate success, perhaps you pick a service, such as outreach

and communications, that is not as daunting initially as incident response. We have success stories of national CSIRTs that began by doing public relations, public outreach. You gain the confidence of your stakeholders, your constituents, the people that live in your country, in many cases, simply by being successful at a service. We always say pick one and be good at it. The mentoring framework also enables us to work with national CSIRTs on not only selecting a service, but then if you choose to, how should you go about expanding into other service offerings? Obviously, incident response would be primary, but you cannot force it, right? You have to work with them as to what their skills and their capabilities are. I think that the success we demonstrated in sub-Saharan Africa, we proved ourselves to the United States government because we are now on a global footing. There really is not any region, globally speaking, that the United States government interfaces with where we don't have a stakeholder, a partner, an engagement, primarily being bilateral or regional. And I think a lot of that is because of the framework and how we collaborate with our partners to make them a success.

Suzanne: How many national CSIRTs are there, just to give people an idea of what the global reach is at this point?

Tracy: I do not have the current count, but I know there are roughly over 100 national CSIRTs. There is a new one that we hear about almost weekly or monthly. They are gradually becoming recognized within some of those areas that do not currently have one. The biggest challenge for those that do not have a national CSIRT already is usually resources. Some of the really small locations, not just geography, but population-wise, they are relying on maybe one or two individuals that are functioning as kind of that coordination hub in the absence of a national CSIRT. Just to mention one item that Jamie was talking about, selecting services and starting with one or two services and expanding one of the resources that we use and help teams to select their initial services is the CSIRT Services Framework developed by the Forum of Incident Response and Security Teams, or FIRST. And those resources are available on their website, first.org. And those are very helpful in working with teams to identify what are the needs of their stakeholders and constituents and what services can they provide immediately to help fill some of the gaps that might exist. It is a long list. We do not expect any team to ever perform all of the services. It would probably be almost impossible without a very large staff. But it does help you prioritize your efforts.

Suzanne: Thank you. A hundred is enough to have a global coalition of national CSIRTs, and there is one. Can you talk for a minute about what is

going on with that coalition? I have to imagine that that is a really good opportunity for sharing and for learning about other services that are being provided by a national CSIRT that is doing different things than you do. How do those groups share information? Do you meet regularly? We now have Zoom, so I imagine that is a big part of the equation. How does the SEI collaborate with all of these other countries as part of that national coalition—global coalition? Excuse me.

Tracy: Well, many of the national CSIRTs participate in regional activities. There are regional CERTs that we encourage teams to join so that they're helping others in their region on, they may be facing similar challenges that are unique to their region. But one of the things that we do is since 2006, our team has served as the host and facilitator of the annual technical meeting for CSIRTs with national responsibility, or NatCSIRT for short. It started with just 33 attendees from 17 countries. Now we are averaging over a hundred attendees from about 50 countries or economies. We do not have all of them yet, but we do have a large number that come together. It is held each year in conjunction with the annual FIRST conference. And it provides national CSIRTs an opportunity to share information, tools, techniques, some of their lessons learned, and the strategies that they are using to help address the unique problems that national CSIRTs have. Since it is an invitation-only meeting, that really helps with the information sharing and collaborating as well. It is the opportunity for national CSIRTs to be able to speak openly, candidly with their peers since it is invitation only and the structure of the event and, you know, ensures that some of the things they share is not going to be shared externally without permission. We do allow non-national CSIRTs to present at the event if it is something that is relevant to all national CSIRTs. In fact, we are getting ready for this year's event in June. We have the call for presentations open and you can always find more information about the event on CERT's event page. If you do not make it this year, then perhaps next year those listening can submit a talk.

Suzanne: And we will also make sure that those kinds of links are in our transcript for people as well. They will have that. I think that would be a fun event to be at, although the thing about doing a lot of these things on security content is I sometimes have trouble sleeping for a couple of nights because I realize just how complex and insecure the world is in many ways. Maybe I should not go to that conference. Anyway, what are the challenges in this type of work, both for the country interested in developing a CSIRT and your team? James talked a little bit about the resource limitations. What are some of the other challenges that come up for either us at the SEI or for the countries that may be interested in developing a national CSIRT?

James: The near-term challenges for any country would be going back to resources, but the resources could be a little more specific in that they have to have dedicated funding. We have worked with countries, national CSIRTs, where they have not had dedicated funding, and you will go there for one visit and they have got 12 employees, and you will go there for the next visit, and they have got two. That kind of a change, which is called dramatic change in personnel strength, is very difficult to overcome, right, because you are going to train with a group of people only to find that they are not there. Here again, you know, picking a service is very important. Having legitimacy, which in many cases means that you have a national cyber strategy or legislation that legitimizes the national CSIRT as just that, the national CSIRT. Because if they do not have the legitimacy, then if they try to work an incident, does anyone have to work with them? Does anyone have to answer the phone, for lack of a better term, or respond to the inquiry? And in certain countries that we have worked in, they do not. The flip side of that would be that in some countries, they are, in fact, the regulator, which makes it almost equally as challenging because then some people are concerned about working with you because you are, in fact, the regulator and there are legalities there. I think for the folks that make up our team, those types of challenges would be the same for us, right? If we go somewhere and we have worked with you and then no one is there when we come back, well, that is hard. If we go somewhere and they have moved your facility yet again where you were actually in a facility that was conducive to the work that you are supposed to do, but the next time you are basically just in a cubicle farm, that is not quite the same thing. And if we go somewhere and you had computer equipment that was provided by the government, but perhaps now you are working on your personal computer, well, that is not going to help us either. And if you are going someplace and it is a lot of interns or college students, well, they graduate or they are not going to be interns forever. You can also run into problems if you contract heavily for your personnel. I think the other thing that is always challenging to our team is there are cultural nuances that you have to be very attuned to. If we work in areas of Europe, such as the Western Balkans, there are just cultural aspects of that work. And you have to make sure that you do your own research and that you understand what those are. By the same token, we have had people that have gone to Tbilisi, Georgia, and, you know, they are invited to sword dances and, you know, they are offered the local products, for lack of a better term, you know, treated very well. I think Tracy and I have experienced that everywhere. You know, you can also be treated extremely well and, you know, asked to participate in things that are not just always work related. That is good. I would never want to make light of the fact of the travel that

the folks do. There is, you know, significant travel and very long flights.

Suzanne: Yes. I cannot do the long flights like I used to. I used to do the trips to Australia and, you know, Asia and stuff. I cannot even envision that right now. But a lot of the people that work in this area are people that are in their sort of mid-career. They have got experience. But they are still young enough to be able to handle the long hours and some of the local products, as it were. You have talked a little bit about things that we do to help transition this idea into practice. You have talked about the mentoring framework. You have also talked about the resource framework. But beyond those things, what are some of the resources that are available for countries, possibly other smaller government entities that want to either stand up their own national CSIRT or just increase their incident response ability in general? They may have started out with just a single service and didn't even know about all the different services in the framework. What are some of the other resources that people should be aware of?

Tracy: As much as we would love to help every team that needs it, it is, you know, just not feasible. We do have a lot of reference materials on our site such as the *Handbook for CSIRTs*. We also, Jamie and I, drafted a booklet on enabling the sustainability and success of a national CSIRT. A lot of the challenges that Jamie talked about and some of the key things that national CSIRTs have to take into consideration when they are either standing up or selecting new services and other functions that they have to provide is a good booklet and starting point for identifying some of the lessons learned from other national CSIRTs that have been doing it for a very long time. That also contains some additional resources for teams to look at. But also, as I mentioned earlier, getting connected with those regional entities is a great asset and resource for national CSIRTs. So regional CERTs such as Africa CERT and Asia Pacific CERT can help them get plugged in with other teams in the region and to be able to share information, not just when there is an incident, but training opportunities and things of that nature. And then, of course, one of the milestones that we always include in development roadmaps is to join first as a member team, because then that helps them integrate internationally. Not just with other national teams, but CSIRTs and security teams from around the world. There are additional events and training opportunities that they are opened up to as members. Then there is just that added place where they can identify who to contact during an incident. One of the first missions is to be able to be a directory of incident response and security teams. That is a great resource for national CSIRTs in addition to the ones that we provide.

Suzanne: My guess is that there is still work to do, either in transition mechanisms or other things. What is next for you and your team in incident response? And what am I going to be talking to you about in a few months?

James: I think the biggest thing that the team has begun to move towards is in many cases we see national CSIRTs becoming national cyber centers. Here again, no national cyber center is the same, but the broad picture would be that national cyber centers are focused on the cyber ecosystem of a nation-state. By that, I would mean that they are looking at bringing in sectors, or what could also be called critical infrastructure, into the cyber ecosystem that is the responsibility of the national cyber center. I think the aspect of this work that I find very interesting is you cannot come to it with a U.S. perspective, in that we would say, *it has got to be finance and it has got to be transportation*. The nuance here is that you need to work with your partner because they have to determine what is their critical infrastructure. One of the places Tracy has been is Fiji, one of the Pacific island nations, they have three things that I am aware of that they have identified as critical infrastructure. It is the harbor, tourism, and the telecommunications cable that connects them to the world. If you want to stand in front of them and disagree, you can, but to me, you should not, right, because they took the time and the diligence to determine what was critical infrastructure. Another one would be Kenya. Education is considered critical infrastructure in Kenya. It is not just a U.S. or a Western perspective on what is critical infrastructure. And I think the other thing that is interesting in these national cyber centers is how do they want to interact with these sectors. The sector itself could have an incident response or security operations team or cell, or the national cyber center could have people that focus on that area that occupy positions or seats or have interface capabilities within that national cyber center. But the bottom line would be that it is the intent to have a broader picture of the cyber ecosystem of a country and to also have the ability to collaborate, coordinate, and share information across and amongst those sectors. I think that is one of the areas that we are seeing ourselves start to work in, that is quite interesting, quite dynamic. And then everyone likes to talk about AI [artificial intelligence]. But AI will have a role in incident response to me, and that will be with, since we do work with so many teams that are resource-constrained, right, that do not have the ability to have lots of people, if they only have small teams, these small teams will look to AI to augment what we would call eyeball time, right? How long do I really have to look at something? And if there is something that can make that shorter or that can eliminate my eyeball time, they will start to look into that and they will start to implement it in the future.

Suzanne: All right. I look forward to those conversations in the future because I would not have picked tourism as a critical infrastructure, but I can, you know, if I think about it for a little bit, I can certainly see for a nation like that where it actually would be. I really appreciate that perspective of we need to bring an open perspective to what people need to do with these national cyber centers. Tracy, did you want to add anything, or did James sort of take care of that for you?

Tracy: Yes, I think that was good.

Suzanne: Tracy and James, I want to thank both of you for talking with us today. I think it is fascinating how we are interacting more with the world and both bringing our perspective and bringing other perspectives back from out in the world to our work. I find this to be a very exciting kind of thing that CERT is doing. I look forward to some of the things that you are talking about in the future, and I hope that some of our listeners will actually be able to use some of the resources that you have gotten and put together so that they can actually build their own national CSIRT. As I said earlier, we are going to include links in the transcript to all of the resources that we mentioned during this podcast. Finally, I need to remind our audience that our podcasts are available every place you download podcasts, as well as the SEI's YouTube channel. Feel free to give us a thumbs up if you like what you see or hear today. We always enjoy interacting with our audience, and I want to thank you both again for joining us today. And good luck with your next trip to wherever it is going to be because it is not going to be in the U.S., most likely.

Tracy: Thanks for having us.

Thanks for joining us. This episode is available where you download podcasts, including SoundCloud, TuneIn radio, 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 do not hesitate to email us at info@sei.cmu.edu. Thank you.