Establishing a National Computer Security Incident Response Team (CSIRT)
Transcript

Part 1: The Role of a National CSIRT

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 John Haller, a member of CERT's Resilience Enterprise Management Team. I'd also like to welcome back Jeff Carpenter, who is a member of CERT's Coordination Center.

Today, John, Jeff, and I will be kicking around some ideas, offering our listeners some advice and recommendations on the actions necessary to create a computer security incident management capability, not just within an organization, but with national responsibility. And sometimes we refer to these as national CSIRTs, C-S-I-R-T, Computer Security Incident Response Teams. So welcome John, glad to have you with us today.

John Haller: It's nice to be with you.

Julia Allen: And Jeff, thanks for coming back and joining us again.

Jeff Carpenter: It's good to be back, Julia.

Julia Allen: Okay, so I think Jeff, I'll toss the first ball to you. So why don't you get us started in describing why would a nation, why would a country, want to create a national CSIRT? Generally what problems are they trying to solve by standing a team up?

Jeff Carpenter: Well, a national CSIRT, distinct from an ordinary CSIRT that may exist in an individual company, a national CSIRT is unique because its focus is on how, from a cyber perspective, to protect national and economic security, the ongoing operations of a government, and the ability for critical infrastructure to continue to function. So they focus specifically on the issues that a government is concerned about for the operation and continuance of the country from a cyber perspective.

John Haller: Yes, and just to and to echo what Jeff said, I mean I think the national CSIRT really offers the government an organizational form to do some of the critical capabilities for cyber security.

So for instance, monitoring incidents at a national level or identifying those incidents that would really affect critical infrastructure or say, affect defense or the economy, to warn the nation, to warn critical stakeholders about computer security threats, be those viruses or vulnerabilities or what have you. And in some respects, to help build potentially organizational CSIRTs within the nation to help the various institutions in the country find their own solutions for computer security.

Julia Allen: So would it be fair to say that one of the roles of a national CSIRT is to connect the dots? Because you've got often in many countries, you have the private sector holding onto or being responsible for various parts of the national infrastructure, but there's really nobody that's responsible for a national strategy, kind of helping all the pieces fit together. Would it be fair to say that that is also one of the reasons why you might want to have such a capability? John or Jeff?

John Haller: I think so. I mean, I think that in many cases, I should mention infrastructure is not held by the government. Critical infrastructure may be held by companies or private firms. And it's part of reaching out to critical infrastructure, for instance, and facilitating an exchange of information to identify threats, to identify, for instance, just to define assets, just to figure out, for the government to figure out what are the critical systems or critical software that are vital to, for instance, national economy or very important sectors of the economy. And that's a little bit distinct from let's say a regulatory body where they're strictly looking to enforce certain standards within the economy.

Julia Allen: Great, thank you John, very much. So Jeff, what are typically some of the key elements or key aspects of the mission for a national CSIRT? We have a general ideal what one is about and what their purpose and objective is. But what are some of their mission statements or elements that they have to worry about?

Jeff Carpenter: Well, when you look at the term CSIRT, incident response is part of that acronym. And the teams don't only do incident response but we start by talking about incident response because that is an important component of what these teams do.

And when we talk about incident response, we're concerned about incident response in cases where the incidents have some significance. So we're looking at incident response in cases where we have crime involved, espionage, economic espionage, or terrorism. Those are generally the four groups that a national CSIRT is primarily interested in.

So they need to build a capability to receive incident information, analyze that information and determine does it meet that level of significance. Does it meet, does that activity match up with one of those four categories? And then correlate the information that they're getting from multiple sources so that they can get an understanding of what's actually happening and then be able to work with the critical infrastructure in government to provide advice to those entities that are important to them, their constituents, on how to protect themselves from that activity, how to defend themselves from that activity. And in the case where they might have been compromised, how to recover from that activity.

Beyond incident response, there are a number of other types of activities which a national CSIRT is involved with. They tend to be the international point of contact for their country from an incident perspective. So they work with their peers in other countries. But they also collaborate extensively within their country with law enforcement, intelligence, government, critical infrastructure.

Julia Allen: Okay. And any other elements you wanted to highlight Jeff?

Jeff Carpenter: I think one other thing that's worth mentioning is they also help with the readiness of the government to respond to incidents by conducting exercises. So in many cases, they -- either they lead or play a significant function in helping organize an exercise to test the capability of the government and critical infrastructure to be able to respond to and handle an incident that would have national significance.

Julia Allen: Excellent, excellent. So John, we're going to move into more of the specifics of establishing a national CSIRT. So could you start us off? I notice from your reports and presentations that you identify four strategic goals for a national CSIRT. Could you just introduce those by name and then we'll dig into each one individually?

John Haller: Sure. The first one we looked at is planning and establishing a security incident management capability. So this is basically standing up an organization that will conduct these functions, determining what your constraints are, getting it funded and so forth. The second is establishing situational awareness, so what you have to do to become aware of security incidents in a country. The third is managing cyber incidents, what are some of the overall steps you have to do to successfully manage them? And echoing what Jeff said, the last one is supporting the national cyber security strategy -- making sure or ensuring that the national CSIRT is really contributing to the national strategy and the concerns of the nation.

Part 2: Goal 1 – Plan and Establish a CSIRT Capability

Julia Allen: Okay, so let's walk through these. Your first one was the actions involved in planning and establishing a national CSIRT. So what are some of the things involved in meeting this goal?

John Haller: Well, the first is -- they're all co-equally important -- but the first is talking to your major stakeholders in the government and potentially in industry to make sure there's some alignment between the government's expectations and the expectations or the operations of the national CSIRT. So starting that conversation early to ensure that as the organization or the capability is stood up that the government knows what it's doing and that it's supporting what critical stakeholders feel is important.

In addition, sort of a survey or a look at what the constraints are. So many nations are in different situations in terms or have different capabilities to staff an organization like this or to fund an organization like this. So you really have to understand what your constraints are just in terms of staffing or the technical expertise that may be available to you when you start to build a capability like this.

Jeff Carpenter: One question we get a lot is where do you put the national CSIRT? Is it in government? Is it outside government? And our advice has always been every country is different in terms of their, how their government's organized, how their culture operates. They need to make those decisions themselves based on what fits.

But we're seeing a trend that because the emphasis on national CSIRTs over the past decade has increased from a national security, economic security perspective, governments are realizing that there are certain components of a national CSIRT that really have to be inside government to ensure that the national security and economic security issues are adequately addressed. So we're seeing in a lot of countries where national CSIRTs might have existed outside of government, they're either being moved into government or the responsibilities are being divided between government and the private sector so that there is a component or is a national CSIRT component that's within government.

Julia Allen: So Jeff, when you say within government, I mean that's a broad organizational structure. Do you find, other than the standard "it depends" response, do you find that there are government agencies or offices or functions where the national CSIRT tends to fit best?

Jeff Carpenter: It varies across countries. But I think the most common government agencies would be some type of a commerce department that deals with industry is one. Telecommunications regulatory agency is another common one. In countries that have an interior department or an interior ministry. Those three are probably the most common locations. But there are other countries where it appears in a law enforcement-type organization or a legal, like an attorney general- type department as well. But I would say commerce, interior, telecommunications are probably the most likely places where you would find one.

Julia Allen: Okay. And John, did you have further points you wanted to make in terms of the planning goal?

John Haller: Well, an additional one is determining the authority of the national CSIRT, whether the national CSIRT would have authority over the community. So for instance, you could break that down either authority over government operations and the government's use of information technology or authority over the public's use of the internet.

Now, and I think Jeff would echo this, usually national CSIRTs function better and are more effective when they act in an advisory capacity, not in any type of regulatory or authority role. Usually where they work and coordinate especially with everybody in an unbiased fashion, they're a little bit more effective. But that's another part of -- goes along with determining the structure of where the national CSIRT fits.

Part 3: Goals 2, 3 – Build Situational Awareness; Manage Incidents

Julia Allen: Great. Okay, so you said the second goal is around situational awareness. So we'll talk about that next. So how might a new national CSIRT manage incidents, become situationally aware, particularly as Jeff said, of the ones that are most important, and if part of their mission is to make citizens aware of the incident and their other services and capabilities, how does that all play together around situational awareness?

John Haller: Well probably the key, the key part of situational awareness is trust, where most national CSIRTs are really working cooperatively with organizations in the country to learn information about computer security incidents or cyber crime or other types of crimes involving computers. And it's really critical that the national CSIRT develop trust so that different stakeholders in the community are willing to give that information to the national CSIRT. If they don't trust you, they're probably not going to hand over their sensitive information.

I mean frequently, the computer security incidents or the cyber crime is frankly embarrassing or it may have to do with security vulnerabilities on the part of the individual organizations. So trust is key and building trust is kind of complicated. I mean, maybe not complicated but can take some time. It involves good personal relationships between the leaders involved. It involves good policies and procedures surrounding information.

So if I'm in the position of someone in industry who's in critical infrastructure, and I'm going to tell this national CSIRT all about my vulnerabilities or some incident that happened, I need to be assured or have some assurance that my information will be adequately protected. Part of it also involves just coordinating with stakeholders in the economy. So what are they experiencing? And when they do experience incidents, coordinating and putting -- getting the right information for those stakeholders or for industry or whoever the victim of an incident is, getting the right information to them so that the damages can be mitigated or the incident can be responded to.

A big part of this, and maybe one of the more challenging parts of this, is really determining which incidents are important. So as Jeff alluded to, it's really incidents that are of critical nature to the nation or to the economy. But frequently, national CSIRTs when they first open up or they're first taking incidents, are deluged, are inundated with people having computer problems, people experiencing something where maybe there's already been a solution or a patch to it. And the national CSIRT needs to have some way of identifying what those incidents are that are really critical to the nation or to the economy or national defense, what have you.

And there's a bit of a dual role in there, where their primary responsibility is to critical infrastructure, nationally important organizations. But they also fill a role where they're warning and advising the public on how to use the internet more safely, on how not to have their computer compromised or experience viruses, or what have you. So there's kind of a dual role there. But really identifying the incidents that are important is really critical.

Julia Allen: So would you say then clearly you want to focus the resources on the critical incidents. But you also mentioned and Jeff did as well, this education and awareness activity, building up community knowledge. So I would expect like a robust web presence, where you point people, like frequently asked questions and other kinds of things where you allow your constituents who are having localized problems to have some resources to draw upon, correct?

John Haller: Oh, absolutely. I mean, really, there's a couple sides to that. First of all, as far as the nuts and bolts of how the national CSIRT operates, there needs to be some intake mechanism. In other words, some way that incidents can be reported, whether that's a web presence or a form or a properly managed email account, or what have you.

And then in addition, particularly with regard to a national alert and warning and letting people know about vulnerabilities and problems, there definitely needs to be a web page or some way to communicate concerning best practices, lessons learned from incidents, the next step, steps that people can take to protect themselves when they use the internet and so forth. And I mean that may be, if the national CSIRT doesn't have that built internally completely, perhaps they can direct people to other resources. But that warning and education piece is really critical.

Julia Allen: And I would imagine -- Jeff mentioned the rich resources that other national CSIRTs provide. So obviously, this problem has been solved in many other countries. So would a new CSIRT be able to draw upon those resources?

Jeff Carpenter: Yes. In fact, one of the things that we do in the CERT Coordination Center is we work with the national CSIRTs around the world to help them collaborate better. We hold an annual technical meeting where we invite the people doing technical work on national CSIRTs from around the world to come together and discuss the unique issues that a national CSIRT faces and work on joint solutions to the problems that they're all facing. And when we first started doing this and brought the countries together, they were all surprised at like, “Hey, these other countries, we're all in the same boat together. We have unique issues to our kind of organization that other organizations don't have. And we can learn from each other and learn from the solutions that other teams have developed.”

Julia Allen: Excellent.

John Haller: That's where that coordination piece is huge, is really key. You may not have the capability or the capacity to do certain things internally. But if you can coordinate successfully

and participate in some of the community meetings that I think Jeff is going to talk about, you can really reach out to some of the other national teams that are in existence.

Julia Allen: So John, before we move on to the next goal, is there anything else in both the national CSIRT becoming situationally aware and their role to make the citizenry aware, are there any other points you wanted to make in that goal area?

John Haller: Well, and at base level, national CSIRTs need to have some type of analytical capability, some ability to analyze incidents -- and Jeff alluded to this as well -- where that may be a fairly basic analysis. I mean, it may be a triage, for instance, do I care about this incident or not? But ideally, the national CSIRT at least needs to look at incidents and inform their major stakeholders, whether it's the government or critical infrastructure, inform those stakeholders about the meaning of the incidents. But I mean, I think we've basically covered it.

Part 4: Goal 4 – Support the National Cyber Security Strategy

Julia Allen: What actions can a national CSIRT take to support, if the nation does have a national cyber security strategy, how does the national CSIRT play into that?

John Haller: Well, I mean the first thing is the nation may not have really put together a cyber security strategy. So there may be, frequently there are situations where the national CSIRT is developing at the same time that the national cyber security strategy is developing. Or it may be that the national CSIRT is developed and built and then only a couple years later or years later, the government finally decides, "Well, let's have a really well-rounded cyber security strategy." So I mean in that case, the sponsors or the champions of the national CSIRT, the people who are pushing it from the inception, from the start, they really need to talk to the government, talk to people in the government, and bring about these issues and discuss these issues from the start. And that's for a couple reasons.

First, they may need to really educate people in the government about the importance of cyber security, about the extent to which critical systems and critical infrastructure are dependent on ICT, on information and communications technology. And they may really need to educate about the importance of cyber. And in addition, they need to talk to critical stakeholders early and often, so that they are supporting the institutions or the parts of the economy that are really important to the nation. So in many cases, this will be an iterative or an ongoing process of developing a strategy and developing the incident management capability. Now, assuming there's a strategy or something approaching a strategy, the other major area where a national CSIRT can contribute is helping the government understand cyber from a policy and legislative perspective. In other words, how do different pieces of legislation or regulation affect cyber security, and how does cyber security affect what the government does? That may be in terms of regulation. It may also be in terms of information systems that the government is looking to use or maybe purchase or something like that. The national CSIRT can help the government partner with private industry or different critical infrastructure providers. They can help the flow of information by facilitating working groups. In other words, getting people in the government together with people in industry, in a neutral environment, to talk about security and to talk about vulnerabilities. They can help enhance the cyber security strategy or national cyber security by helping organizations build their own CSIRTs.

Julia Allen: Okay. You both have mentioned this idea of a champion or a sponsor of the national CSIRT, particularly in countries that are just trying to get started. Comparable to my question about is there a typical government agency where CSIRTs live, is there a profile of a champion or a sponsor or the group or individual who seems to be the catalyst for getting a

national CSIRT on the agenda? Jeff, what do you see in your work with the other national CSIRTs? Any ideas there?

Jeff Carpenter: There's probably two main areas where we've seen champions come from. One is from a government agency -- someone who has some sort of technology management responsibility within the government. And they recognize, because of the infrastructure that they have to protect, that there's a need for the country to have that kind of capability and they begin the dialogues to do that. We've also seen from outside of government a lead academic in the country, who is focused either on technology or even potentially on security issues, will advocate to the government that they need to begin to look at that kind of a capability. Certainly in some countries, it's been other people. But I think those two groups are probably the most common when you're starting out from a government that has not really looked at the issue in-depth previously.

Julia Allen: Okay. So before we come to our close for both you Jeff and John, if I had a passionate group within my country that wanted to get a CSIRT started, do you have a first couple of steps that you've seen have worked well to help get a national CSIRT initiative off the ground? Kind of the first one, two, three steps?

John Haller: Well, I mean I would say the first is probably talk to the other teams and participate in some of the various forums surrounding national incident management to get the input of other people who have been in a similar situation. I think looking at your constraints and getting a realistic picture of what you have to work with is very beneficial. And finally, start talking to your government, the critical leaders in various infrastructure in the economy and determine what they see as the need. I don't know if Jeff would have additional ones or other ones, but I think those three are probably to my mind the initial three.

Julia Allen: Jeff?

Jeff Carpenter: I think those are a good three to start.

Julia Allen: Okay. Well Jeff, could you bring us to a nice close by perhaps pointing to some resources where our listeners can gain more information?

Jeff Carpenter: On the CERT's website, we have a page dedicated to national CSIRTs, where both countries that are looking at creating a national CSIRT can get information, and we also have information useful to existing national CSIRTs. We also have information I mentioned about the national meeting that we -- the annual meeting that we have each year. We have information about that meeting and other tools that we have available to help national CSIRTs collaborate with each other. But there are some other organizations as well that can be helpful to national CSIRTs. FIRST, the Forum of Incident Response and Security Teams, which is an international organization focused on incident response and how to help organizations that have incident response teams build their capabilities. That team, that organization, it can be of help.

And also, there are some regional organizations around the world that have done a lot of work to help countries in their region create national CSIRT capability. So probably the one that has done the most work in that area is ENISA (European Network and Information Security Agency) in Europe. But we also have APCERT in the Asia Pacific region and GCC in the Middle East. Those organizations, if you're located in one of those regions, in many cases they have people from other established teams come and actually come to your country and can work with you and help you get capabilities created.

Julia Allen: Excellent. Well, John, thank you so much for arranging for us all to get together to start what I think will be a great series of podcasts on standing up national CSIRTs, so I appreciate your time today.

John Haller: Sure, it was my pleasure.

Julia Allen: And Jeff, always great to have you back on the series. Thanks for all your great recommendations and guidance.

Jeff Carpenter: Sure. Thank you, Julia.