Tackling Security at the National Level: A Resource for Leaders
Transcript

Part 1: An Introduction to National CSIRTs

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 security governance and executive outreach. Today I'm pleased to introduce Jeff Carpenter, the technical manager of the CERT Coordination Center. We'll be discussing how business leaders can use national Computer Security Incident Response Teams – we'll refer to those as CSIRTs – as a resource when dealing with global incidents and cyber security issues. So, Jeff, happy to see you, it's nice to be back in Pittsburgh with you.

Jeff Carpenter: Yeah, it's good to see you, too, Julia.

Julia Allen: Great, looking forward to exploring this a little bit and seeing what we can pass on to folks.

Jeff Carpenter: Good.

Julia Allen: Okay, so why don't we start out with some definitions, Jeff? What is a national CSIRT, a Computer Security Incident Response Team, how many are there today, and just roughly, where are they located?

Jeff Carpenter: Well, let me start with the concept of a CSIRT, and that's a, as you mentioned, Computer Security Incident Response Team. And that's generally a team within an organization that helps address incident response, computer security response issues within an organization.

If you look at that at a national level, it has a slightly different focus. National CSIRT is concerned about computer security incidents that are happening within the country, but it's generally interested in large incidents or incidents that can have an impact to the economy, can have an impact to the critical infrastructure, can have an impact to the operations of the government, or have an impact to national security.

Julia Allen: So ones that are more broad than maybe just a single organization?

Jeff Carpenter: Right, so they're looking at things that can affect many organizations within their constituency. And they're also concerned about activity that's happening in their country that can have either an impact in other countries, or activity that's occurring in other countries that can have an impact in their country. So there's cooperation between the national CSIRTs in solving problems that go across borders.

Julia Allen: So, about how many are there, and kind of roughly geographically where are they located?

Jeff Carpenter: National CSIRTs, there's probably about thirty to fifty today in varying stages of capability and maturity. Most of them are located in the Americas, in Asia, and in the European region.

The largest area that doesn't have national CSIRTs is the African continent. That's pretty unrepresented, and until the past couple of years the Middle East was the other large area; however, now the Middle East we're beginning to see some activity in Qatar and Saudi Arabia and the United Arab Emirates where they are now forming national response teams in the Middle East. So now that the Middle East, which was one of the largest areas that was underrepresented, is being tackled, Africa is the next major region that doesn't have national CSIRT teams.

Julia Allen: I can envision that given that the Internet's global, given that we're all globally interconnected, that this capability of a nation or a country to have some kind of incident response capability is really key when you're trying to coordinate an incident worldwide.

Jeff Carpenter: There's several reasons why there's an interest for countries to have national CSIRTs in other countries. Certainly in the United States we would want to have a national CSIRT in the United States, and we do, US-CERT, but it's also in our interest to have national CSIRTs in other countries for several reasons.

One reason is because, as I mentioned before, you can be the victim of activity that either originates in another country or passed through – you know, there's a pass-through for that country to your country. And it's helpful to be able to communicate with someone in that country who might be able to help address the situation – either stop the activity or engage law enforcement, whatever's appropriate in that circumstance.

Julia Allen: Well, and just from the reading and some of the research that I've done, it appears as though some countries are more susceptible to having very active and aggressive intruder activity, and so I suspect if that country has or is starting to build a national CSIRT capability, that's in all the other countries' best interests, where some attack might be passing through that intermediary country.

Jeff Carpenter: Right. So one of the roles of a national CSIRT is education, to help educate people as to what the problem is and what they need to do to help protect themselves. So it's in our interests for people in other countries to be receiving education and do a better job of protecting their assets, so that they themselves are not victims and then as a result of them being victimized having the intruders then turn their attention to attacking people in your country.

Julia Allen: Right.

Jeff Carpenter: That was a little convoluted, but –

Julia Allen: Right, but in other words we're all connected, everybody can pass through everybody, and so if you're not educated, you're vulnerable. You're susceptible to being taken advantage of.

Jeff Carpenter: Right, and as you mentioned, as you look around the world, the technology that's used is slightly different in every country. For example, in Korea, Windows has a much higher penetration rate than it does in the United States. And with different time zones we find that activity that originates can be seen in some countries first before it's made its way to other countries.

So it helps with national CSIRTs being in communication with each other, to let others know that they're seeing activity that hasn't been seen before, to give as much time as possible for other national CSIRTs to prepare for that type of activity.

Part 2: How Business Leaders Can Interact with National CSIRTs

Julia Allen: Let's turn our attention to businesses and business leaders. Why would a business leader care, or how would a business leader take advantage of a national CSIRT capability? How would they use such a capability?

Jeff Carpenter: Well, one of the advantages is the government can have access to information that the businesses might not have access to, for example threat information, knowing that specific industries or companies might be the targets of specific criminal activity.

Additionally, they might be able to provide information on technical vulnerabilities that a company might need to address within their infrastructure, especially if the business is operating in a critical infrastructure where the government is highly dependent on that infrastructure for their own operations.

Julia Allen: So, for example, like telecommunications or the financial services sector?

Jeff Carpenter: Right. Governments generally don't run their own telephone switches, and they don't have their own financial systems. They're dependent on industry to handle those things for them, so it's in the government's interest to work with industry to provide them with information and help them understand what the risks and threats are.

And this all works best when it's done in a proactive manner, so establishing those relationships prior to there being a problem or an incident. So focusing on how can we minimize the potential that a critical infrastructure can be compromised, rather than reacting to it after it's already happened?

Julia Allen: So how would an organization, or how would the leadership of an organization, outreach or reach out to their national CSIRT, and how would you recommend that they build this relationship proactively?

Jeff Carpenter: Well, first they need to find out if their country has a national CSIRT.

Julia Allen: Yeah, that would have to be first, right?

Jeff Carpenter: Right, and if they're not sure, we at the CERT Coordination Center, we have a section of our website dedicated for national CSIRTs, and we have a list of the national CSIRTs that we are aware of with links to their websites to help people get started.

It's also possible that a country could be in the process of forming a national CSIRT. So if someone isn't sure who to contact, some of the good places to start would be contacting national law enforcement, or the national telecommunications regulation authority, or some ministry in the government that handles oversight of Internet service providers. Someone in one of those entities would probably know of the national CSIRT and where it might be located.

Frequently, when a country is starting a national CSIRT, they'll heavily rely upon advice from industry and academia to help get it started, because frequently the people that have the best technical understanding of the problems come from industry and come from academia. So we've

seen in many countries get started, that the government will reach out to industry and academia to help them.

Julia Allen: Now, you had mentioned, or you touched on briefly, this notion of the national CSIRT and law enforcement. How do they differ, and are there times when a business leader would go to their national CSIRT versus go to their law enforcement points of contact?

Jeff Carpenter: Yes, and the specific overlap between them will vary from country to country, but generally law enforcement is focused on finding out who has committed a crime, working to get them arrested, and then bring them ultimately to justice. A national CSIRT is generally more focused on the technical issues involved. How was it done –

Julia Allen: Kind of what methods and techniques were used to compromise the systems?

Jeff Carpenter: Right. How can we determine if we're vulnerable, and if we are, how do we prevent this from happening again? And then, looking at the broader community, "Okay, well, this company was affected by this particular problem. Are there any other companies that might be susceptible to this problem?"

For example, if it was a problem found in an electric company – a piece of equipment that's unique to an electric company – let's talk to the other electric companies and see if they have a similar problem, or let's talk with the vendor, bring the vendor of that product in and bring their expertise in to help solve the problem.

Julia Allen: So I can see that the national CSIRT, like perhaps across a market sector, like you're talking about, an electric power grid or electrical utility providers, could actually help mobilize the community, mobilize the leaders in that community if there's something that's a situation that they particularly have to pay attention to.

Jeff Carpenter: Yes, and I think you asked before how can business leaders get engaged with the national CSIRT? And there's several ways they can do that. There's a number of initiatives in several countries where the national CSIRT will come together with business leaders in an advisory capacity to share issues that they have and to share how – together talk about issues that they need to solve and work on together. And again, that's a proactive thing, let's bring the leaders together with the national CSIRT and see how we can work together better. And that also builds the relationships so that, when there is a problem, people will know each other and they'll know who to call and they'll have more comfort in calling, because –

Julia Allen: Right, they establish a trust relationship –

Jeff Carpenter: Right, because ultimately trust is a key issue in this. You're not going to be as willing to call somebody and tell them that you have a problem that you need assistance with if you have no idea what they're going to do with that information or what's going to happen. So the building of trust is important.

Julia Allen: That's a key point that I wanted to ask you about. Are there considerations or issues that business leaders need to take into account when they're sharing information with a national CSIRT? Certainly, that comes into play when you're sharing information with law enforcement, but what are the sensitivities, or what should a business leader think about before they start sharing their issues and vulnerabilities with the national CSIRT?

Jeff Carpenter: Well, one thing that we recommend that they do is prior to there being a problem, they discuss this issue with their legal counsel. Because there may be specific laws or regulatory requirements which have an impact on what happens to information that's reported to government, or there may be legal or contractual requirements which would prevent the reporting of certain information. So we recommend that that be talked over with legal counsel in advance. Obviously the laws and regulations are going to differ from country to country. In some countries there may be open records laws, such as in the United States the Freedom of Information Act, which might have an impact on information that is reported – the potential for that information to be released.

However, there's several things to consider in that. One is, if you have a particular incident that's occurring, you don't necessarily need to reveal every aspect and detail of that incident in order to get assistance, so you can talk about the technical issues, the technical vulnerability, without revealing exactly who the victim was, how –

Julia Allen: Right, or that it was your most critical customer database that just got compromised, for example.

Jeff Carpenter: Right, and who might be affected and listing the names of the people. So you can get technical assistance without necessarily providing that. In other cases, it may be the case that while information that you provide to them may be sensitive today, three years from now that information will not be sensitive at all. So it's the potential that if you're providing that information and you think it may eventually come out, you may balance that with the need you have to get immediate assistance, and you may be able to make a risk judgment that the potential that information may come out three years from now is not as costly as the problem that I'm facing –

Julia Allen: Right now.

Jeff Carpenter: Right now.

Julia Allen: And isn't it the case that most national CSIRTs do operate under some type of confidentiality or non-disclosure with respect to the people that contact them?

Jeff Carpenter: Yes, and again the legal requirements will differ from country to country, but most national CSIRTs or most governments that set up national CSIRTs recognize that if information – if they're going to be able to work successfully with industry, if the situation was that information that was reported was immediately released publicly, no business is going to work with them. So many have policies, procedures, laws which protect information which is submitted, but again, we recommend that legal counsel be consulted to fully understand what the issues are in your country.

There are some countries where entities are legally required to report information. That's not the case in the United States, but there are countries where even sometimes sectors are required to report certain information about incidents, so that can work both ways.

Part 3: Collaboration Among National CSIRTs - How Business Leaders Can Benefit

Julia Allen: And just by way of closing and bringing us to the end of this great conversation, how have you seen, in your history with the CERT Coordination Center, how have you seen national CSIRTs interact with one another in the case of a major incident? What are some of the transactions that take place, the interactions take place, when they're all trying to solve a common problem? What does that look like from your vantage point?

Jeff Carpenter: The most successful interactions I see are interactions to solve a problem from happening, and those are the things that aren't the flashy things which make it into the news media. When you have a major event, something like what we had with Code Red a couple of years ago, the time it takes to do complete analysis is generally longer than it is for significant pain to be felt by people. So at that point in time, things can be chaotic. There will be communications between national CSIRTs, but you won't see – I don't know how say this –

Julia Allen: It's kind of behind the scenes, right? I get that impression, that people are working together.

Jeff Carpenter: It's behind the scenes, but there's lots of – when you have a major problem that has just erupted, there's lots of different entities which need to communicate with each other to solve the problem. You need to bring the vendors in, you need to bring law enforcement in. That can be a very large job within a country and a very large job internationally. I'd be joking, and it'd be bad for me to say that always goes smoothly. It doesn't when you're in a crisis situation.

Julia Allen: Well yeah, right, you've got different cultures and different regulations and all kinds of different vested interests.

Jeff Carpenter: And you only have so many minutes to make a phone call. You have to choose who you're going to call in what order. So it can be those kinds of crises – while there is cooperation, I don't think it's the best example of cooperation. The best example of cooperation is when we're working to solve a problem before it becomes a major security problem.

Julia Allen: Right, where you have the benefit of time and thoughtful action.

Jeff Carpenter: Right, so we can say, "This is a particular vulnerability, what's the technical solution to solve this? Who is likely to be significantly impacted? How do we get that information to the right people, to make the changes that need to be made? Are there workarounds that can be deployed prior to the vendor developing a solution?" In those cases, I think we can point to our much better examples of success, because we've worked together to solve a problem before it became a problem. And ultimately our success, I think, is measured by the problems that we prevented from happening, rather than how we responded to problems that had significant negative impact to the economy or to people's businesses.

Julia Allen: So, clearly, a lot going on behind the scenes that sometimes never see the light of day, and thank goodness for that.

Jeff Carpenter: Yes.

Julia Allen: So, just by way of closing, it sounds like if business leaders aren't taking advantage of – aren't knowledgeable about and aren't taking advantage of – their national CSIRT capability, it's something that they definitely want to reach out to, because it sounds like it can be a great resource for them in their enterprise security efforts. Were there any points that you wanted to close with that we haven't already touched on?

Jeff Carpenter: Yeah, I think I wanted to mention – so we found that national CSIRTs will tend to focus on one or two primary things that they can help other national CSIRTs on. So, for example, the Brazilian national CSIRT has developed an extensive capability for honeypots, honeypot technology, and they collect a lot of information from their honeypots and they can share that with other national CSIRTs.

In Korea, they have developed an extensive capability for looking for threats on the backbone Internet service providers. They've developed extensive relationships with the backbone Internet service providers to look for real-time threats, and then other national CSIRTs can learn from what they have done.

So I think one of the advantages of national CSIRTs working together is not only just to share information, but to share the resources that they have, and the capabilities that they've developed. It's not really economical to duplicate those infrastructures in every single country, or those capabilities in every single country. So it's imperative that we all work together. As you mentioned at the beginning, the Internet has global impact, it's a global network, it appears all over the world, and we all have to work together to help secure that network.

Julia Allen: Well, I'm so appreciative of your time and your expertise and, just from our work association, your commitment to this effort and helping us all operate both as individuals and as organizations more securely, and I really do thank you for your comments today.

Jeff Carpenter: Thanks, Julia.