CERT Lessons Learned: A Conversation with Rich Pethia, Director of CERT
Transcript

Part 1: CERT History

Julia Allen: Welcome to the CERT 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. I'm pleased to introduce Rich Pethia, director of the CERT program at Carnegie Mellon. Today, we'll be discussing the past, present and future of CERT and Rich's view of the internet security landscape, so welcome, Rich, glad to have you here.

Rich Pethia: Well, I'm glad to be here.

Julia Allen: Yeah.

Rich Pethia: I think we're going to have fun this morning.

Julia Allen: Yeah, this will be great. I'm sure our audience is going to be very interested in hearing what you have to say. So let's go back to the beginning. When you were asked to create CERT, way back in 1988, after the Morris worm, how did you get started, and what were some of the issues that you had to deal with right out of the gate?

Rich Pethia: Sure. One thing I think is important for people to understand is the internet was a very different animal back in 1988 than it is now. Back then, it was still officially called the ARPANET. It only had about 200,000 systems connected, almost all of them in the United States. There was a vision that was going to accelerate the development of the network, but that vision was still mostly paper, not being enacted, and so it was a very young, small community of technologists.

Julia Allen: Right. I mean, it was originally intended just to be an open research network, right?

Rich Pethia: Exactly. It was intended to be an open research network but also to demonstrate the fact that the network could withstand physical attack so that, if any one routing node were to be taken out, the network would recover and route traffic around it. So, even though it had a research purpose and supported a research agenda, it itself was a research project focused on survivable networks.

So we really didn't know what we were getting into because the Morris worm was the first significant security on the network and it had been a small, trusted community. And so we decided, very early on, that there were a couple of key things we would do and then see how the program would evolve over time. One of the first things we decided is we were going to be a service organization. We had no authority. We really couldn't tell anyone to do anything.

Julia Allen: I mean, this all came out of DARPA, right? The Defense Advanced Research Projects Agency...

Rich Pethia: Yes.

Julia Allen: ...at that time?

Rich Pethia: At that time. And, since they were responsible for the network, they believed that they would see future security incidents and they wanted an organization in place to help deal with them. But they made it very clear to us: "You have no authority. You can't tell anybody to do anything. You're going to be successful because you provide services that bring value to the internet."

Julia Allen: So you're there if somebody needs help, but...

Rich Pethia: That's right.

Julia Allen: ...you can't dictate?

Rich Pethia: You can't dictate. So, given that, we decided, first of all, that what we would do is build on our strengths. We were a technical organization. We're housed in the Software Engineering Institute. We know software. We're housed in Carnegie Mellon University. We have, at our disposal, people who are experts in computer science and networking...

Julia Allen: I mean, obviously, DARPA called us for those reasons. They wanted us to stand it up because of our core competency...

Rich Pethia: Exactly right. But we still had options, but we decided, early on, we were going to stick with the technical focus. We were there to provide technical assistance to people who suffered security problems. Help them understand what vulnerabilities were exploited if they had a problem. Help them understand how to diagnose the extent of the problem, how deeply they'd been penetrated, how many systems had been penetrated, and then give them technical advice on how to repair their systems and restore operations.

Julia Allen: So how did you decide, early on, how people would get in touch with us, with CERT, and how we would manage an increasing demand, once the word got out that we were there?

Rich Pethia: Well, DARPA helped us in terms of the announcement in that, about three weeks after they asked us to do this and we agreed to do it, they issued a press release that announced that the CERT had been formed. They provided contact information with respect to a phone number. And an email address and that press release was released on December the 7th of 1988.

Julia Allen: Kind of an auspicious day.

Rich Pethia: Auspicious day, and we got our first phone call that night. It was from a government lab that was being attacked from someplace overseas. They were having a very difficult time getting the attention of any federal investigators because, still, this was a very young problem. Investigators didn't really know what to do with it. And they asked for our assistance in helping them track down the source of the attack and trying to get it turned off.

So that was one of our first early successes, as we were able to do that. We traced it back to a set of university machines in Europe that were being used. We called the university, we told them what was going on, and they agreed to look into it. They, in fact, found that their machines had been compromised and they corrected the problem and the attacks against the U.S. facility came to an end, at least for a time.

Julia Allen: So how many folks did you have at the CERT end that were prepared to field those kinds of requests and do those kinds of investigations? I mean, that's a pretty sophisticated process.

Rich Pethia: Well, we started with myself as the only full-time CERT employee and five other people who were assigned to the project on a part-time basis. But it wasn't very many months at all until the full-time staff had grown to a group of about seven, and then we've been adding staff ever since as the problem has expanded and the need has grown.

So I think it's been, for us, at least, it was a learning experience. We didn't start with a lot of planning because we really didn't know what to expect but, as we learned, as the phone continued to ring, as the email messages continued to come in, we learned a lot about how to engage the community, how to work with them, the kinds of things people were comfortable with, the kinds of things people weren't comfortable with...

Julia Allen: So give me an example of, kind of, as we went along the way in terms of our early evolution, what kinds of insights we might have had and what actions we took in response to the demands that people were making of us.

Rich Pethia: Sure. One of the things that we believed was true early on and we certainly found that to be very true is just how sensitive the information is that we're dealing with. When people call us to report an attack against their systems, in order for us to help them, we have to suddenly learn very much about who they are, what their mission is, what they're trying to accomplish, and the configuration of their systems. And that's very sensitive information. They effectively give us the keys. In order for us to help them, they have to help us understand how their systems are configured, what their vulnerabilities might be. And so we thought, early on, it was important to be *extremely* careful about how we handled that information. We found out that was, in fact, the case.

Julia Allen: So I take it this lesson applies to anybody who is standing up an incident response team?

Rich Pethia: I think there are three keys to success in any response team, and building the trust and maintaining the trust of the community is one of the ones that is most important and I'll talk about the other two a little bit later as we get into some other topics. But that's something that we've protected. We maintain strict confidentiality of all information that's passed to us with respect to the identity of the victims or particular descriptions of the characteristics of their systems. We do talk about generic attacks, you know, the way the attack technology is evolving. We talk about weaknesses in particular products, but we never talk about an individual organization or its systems.

Similarly, as we came to begin working with law enforcement, as law enforcement began to get involved with these cases, we came to understand just how sensitive that information was and even the fact that there is investigation under way is something that we don't talk about, even if we're participating. So protecting the trust that's placed in us, I think, is an

extremely important factor, and it's one of the smart things that we did early on was to build the procedures to allow us to protect information.

Part 2: CERT Today; Available Resources

Julia Allen: So it sounds like, obviously, there are cases where we have to be very circumspect and very careful working a particular incident but there are also cases which you've alluded to where we want to take what we've learned and try and make that publicly available and help the community at large benefit from our experience. Can you say a little bit about that balance?

Rich Pethia: It's almost always possible to find some way to extract the information and abstract it at a certain level so that it's no longer possible to trace it back to the particular information provider, especially in our case where we literally get thousands of reports on a monthly basis on activity on the internet. It's very difficult, given all the people that we work with, for anyone, once we release information, to trace that back to any particular source. Being able to do that, being able to abstract that information and send it out to the public, we think, is a critical service that all CERT teams need to provide.

This is a constantly changing problem. The vulnerabilities change over time. The threats change over time and the solutions, the things that you have in place that help you defend your systems one year are not going to be adequate to defend your systems the next year because you've changed the technology, you've probably added new components to your system and the threat has changed. There are new actors out there who are attacking systems in new ways, and we all have to maintain a constant understanding and be vigilant to those changes over time.

Julia Allen: So, you know, it sounds like, and I know from my own experience working with a program I've observed, that we've really moved from -- I mean, we still do our reactive incident response and reporting and recovery activities, but I see us also moving into much more of a strategic direction. Can you say a little bit about what you view as CERT's responsibility to the community from kind of an education, training, awareness, outreach, research perspective? I know that your thinking has evolved over time as you've been in this role, and those activities have almost become a bigger part of the program than our typical operational capability.

Rich Pethia: In fact, they have, and this happened for several reasons. First of all, as we, in the early years, worked to help people resolve incidents, we came to understand just how much we did understand about the vulnerabilities that were in the software that we used and the systems we used, the threats, how people were attacking systems, how those attacks changed over time, the increased use of automation, attackers who were now using the internet itself to attack systems that are on the internet. And so we came to learn a lot about the problem, more than a typical system developer would know or more than a typical...

Julia Allen: The typical IT organization...

Rich Pethia: ...IT organization would know because we were literally living in it day by day and watching it change over time. Capturing what we'd learned and finding ways to help people use that information in a way that allowed them to better protect their systems was something that we thought was critical, so let me give you a couple of quick examples. Very early on, as we got reports in from organizations that had their systems compromised, it

became very clear that many organizations really didn't understand how to put even the most basic security policies and security management practices in place.

Julia Allen: So, in other words, you were seeing the same thing occurring across a wide range of organizations, regardless of what market sector they were in, for example?

Rich Pethia: Exactly. When we got reports in, we didn't see 500 different kinds of incidents, we saw the same kind -- we saw one incident type repeating 500 times. And so that's one of the earliest things we began to produce was something we called and still do today Tech Tips, simple guidelines that help organizations understand how to put practices in place to help them deal with particular problems. And that evolved over time. Now, we have an entire suite of courses that we make available to organizations. We have guidebooks and textbooks that have been published to help people understand how to put the right kind of security policies and practices in place, and that was, you know, an early example of trying to capture lessons learned and make them available to the community.

Part 3: Progress and Promising Solutions

Julia Allen: That's really terrific. So, you know, there's obviously been a lot going on in the program but let's, if we can, just turn our attention to what folks can do with everything that the program has developed. You know, from your vantage point, if you were an executive or a business leader in an organization today, you know, how would you take advantage of what CERT has provided and stay connected and benefit from, you know, this government investment and this capability?

Rich Pethia: One of the things that we firmly believe is that this is going to be an ever-changing problem and that it's going to require attention across what I'll call the entire system or software lifecycle. So, when you talk about leaders of organizations, there are different kinds of organizations. There are people who produce technology, who produce software products, the operating systems and the applications. There are people who provide services, IT service providers, internet service providers. There are large corporations that use IT technology in a way that allows them to achieve their business goals and there are certainly individual users, both in the corporate sense but also home users. And all of those individuals, leading whatever it is that they're leading, really have a role to play in helping the nation deal with this problem.

Julia Allen: Right. Because, I mean, the adage is, you know, when you're connected to the internet, the internet's connected to you, so it doesn't matter who you are or where you are, you're a point of vulnerability if you're not protecting yourself.

Rich Pethia: That's right. And you're also, if you're a technology developer, you're putting products into a hostile environment, and you need to understand that those products are going to be attacked. Not might be attacked -- they will be attacked. So we think, for example, technology producers need to focus on producing more secure products, products that are able to withstand the threat that's out there today or the threat that may be there tomorrow through stronger security features and also higher-quality implementations. We often see cases where a product, even though it has a sound security design, it has the right security mechanisms built in for the kind of functionality it's trying to provide, it's often vulnerable to attack because the implementation is weak. Bugs in the software. Everybody's heard about the classic buffer overflow, and we've been hearing about this coding problem for 15 years.

Julia Allen: Right, forever.

Rich Pethia: And it's persistent, but it's the kind of low-level implementation problem that allows software to be attacked successfully by attackers.

Julia Allen: So if I were a technology solution provider, what are my incentives for addressing buffer overflows in my products, just as one example?

Rich Pethia: The incentive, I think, is pretty simple, and that is it is actually more cost effective for a technology producer to find and eliminate these kinds of problems while a product is in development than after the product has been deployed to the field. Correcting these problems once -- and we've known this from the history of software engineering for years -- correcting these problems after the fact is a very expensive process. Engineers have to be taken off development projects, customers have to be contacted, patches have to be created. They have to be tested, and that whole retrofit process is...

Julia Allen: Right, so it's costing...

Rich Pethia: ...very expensive.

Julia Allen: It's costing them a lot more dealing with it when it's a deployed product versus a product in development?

Rich Pethia: Exactly. Exactly. Similarly with service providers. I think we've seen a trend, especially in the last four years, where more and more internet service providers are providing security services to their customers so you, the home user, may not know much about firewalls, the need for firewalls or may not know much about the need for antivirus software but, very often today, your internet service provider does and they will package that up as part of the product and the service they make available to you, and we think that trend needs to continue as the threats continue to change.

Julia Allen: Right. I mean, it's kind of -- I always equate it, when I'm talking to someone who's not very literate about computers, is it's like driving a car and having the car manufacturer expect you to know how every aspect of the engine works. We, in the security community, I think, are still at the stage where we're expecting our users to know how to manage and configure firewalls, to know how to do antivirus, and so I agree with you. I hope this trend with the service providers continues because people, when they use a computer, they don't want to have to worry about that.

Rich Pethia: That's right, and I think it's also a lesson to be learned by the technology producers themselves. Building a human interface to their product that is simple for the average user to use, and use successfully from a security standpoint, is the kind of improvement I think that was very important and something that I hope the industry begins to move towards.

Julia Allen: Okay. Is there one last maybe category of producer you want to talk about?

Rich Pethia: I think the other one is the system operator, the corporations, the big IT shops in medium, large, small corporations really need to understand that they have to put enterprise-wide security programs in place in order to successfully deal with a threat, ensuring that everyone in the organization understands what the policies are to protect systems, so that they understand what their roles are with respect to enforcing those policies

or using those policies, ensuring that people are trained so they understand how to do the things they need to do. How do you set up accounts in a secure fashion? How do you manage those accounts over time? You the individual user, what are your responsibilities with respect to protecting information, protecting your account information, your passwords, what have you? And certainly what is your role as an individual user with respect to reporting anomalies or possible security problems that you see? We see many problems that go on for months and months, simply because the individual users don't feel the responsibility to report them.

Julia Allen: Or don't know who to report them to.

Rich Pethia: Or don't know who to report them to. So having that real enterprise-wide view of security that ensures that all the players understand what their specific roles and responsibilities are we think is very important.

Part 4: What Should Leaders Do?

Julia Allen: So, as a business leader, responsible for putting such a program in place, what would you say are a couple of really key critical things that I can do to enable an enterprise-wide security program?

Rich Pethia: First of all, as a leader, is to show commitment and support to the entire effort. We have seen many cases where the senior executives believe that "that security stuff" is for somebody else, but they're very happy to share their account information and their passwords with their administrative staff so they can handle the email for them. So, number one, help the organization understand that this is something that's really important, that you're committed to enforce the corporate policies, and that you live by those.

Julia Allen: Right. In other words, that you're an example of what you're trying to enforce.

Rich Pethia: Right. Walking the talk we think is especially important. Coming to understand, allowing your IT staff to have the time to really understand what good policy and good practice looks like, which means investing in building skills and capability in those people. We see, again, many people in the IT world who would love to do a better job of security but they don't know quite what to do and they don't have time to do it. There are too many other demands on them.

So ensuring that the budget is adequate to support these kinds of activities is important, and then, once practices are put in place, making sure that they're enforced. If there is an infraction of security rules, even if it's done by the most productive employee in the company, you have to enforce them; otherwise, they won't last. People won't believe that you're serious and, over time, we know that security left unattended degrades and you'll very quickly go from a highly secure position to a very insecure position because of lack of attention to the hundreds and hundreds of details that you have to pay attention to on a daily basis.

Julia Allen: Yeah, a fairly daunting undertaking in the face of everything else that a business leader has to consider. So, obviously, getting these all woven into the framework and the day-to-day processes of the organization is really, I think, really key to making it happen.

Rich Pethia: Yeah, I agree. Just like other key business processes or something that organizations learn to live, they also need to learn to live the security policies and practices

they put in place. This problem is not going to go away. It's only going to get worse over time or, at best, it's going to change over time but it's not going to go away. Now that the bad guys know there's real money to be made by attacking systems, unfortunately, as with other parts of the society, those bad guys are going to be with us for a long, long time to come.

Julia Allen: How would you like to see business leaders who are trying to run small, medium, large enterprises take advantage of what CERT has to offer, and, you know, how would you guide them to stay up to date with our developments?

Rich Pethia: Sure. Well, first of all, I'd like to invite everybody to visit our website, both the SEI website, sei.cmu.edu, and the CERT website, cert.org, and take advantage of the many publications that we make available on a regular basis. We have methodologies that are available that people can just pick up and use with respect to doing comprehensive risk assessments for their organizations. We have a number of courses that we make available routinely on a public basis. And so if they have ongoing questions, contact us through the SEI's customer service organization.

Julia Allen: And I understand that there's also a worldwide network of computer security incident response teams, you know, around the globe, obviously many of those we helped established, that can also serve as resources for people in different countries or different regions.

Rich Pethia: Right. One of the early -- well, in fact, one of the objectives that we were given by DARPA, way back when we started CERT, was to serve as a model to help other organizations build their own incident response capability, be that at a large corporate level or even at a national level, and so there are now over 200 incident response teams worldwide. Many of them work together through an organization that we helped create. It's called the FIRST, the Forum of Incident Response and Security Teams. Its web address is first.org.

Julia Allen: So folks don't need to start back in 1988 where we started?

Rich Pethia: No, no. We can leapfrog you ahead of all that misery that we went through, and there are some examples of very effective things that organizations can do, and I think people would be wise to take advantage of all that learning.

Julia Allen: Well, Rich, thank you for your time today, and I look forward to talking with you again.

Rich Pethia: Thank you.