Tackling Tough Challenges: Insights from CERT's Director Rich Pethia
Transcript

Part 1: Looking Back, Looking Forward: The Good, The Bad and The Ugly

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 software assurance. Today I'm pleased to welcome back Rich Pethia, director of the SEI's CERT Program at Carnegie Mellon. Today Rich and I will be discussing the current and future state of Internet security, and CERT's role in tackling some of the very tough challenges we all face as CERT celebrates its 20th anniversary. So welcome back Rich, really glad to have you with us today.

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

Julia Allen: Well you have a particularly unique vantage point: CERT's vision of a securely connected world; our mission of enabling informed trust and confidence in the use of information technology; and certainly given your access to government, commercial, and academic leaders. So what do you see as the current state of the Internet and information security, and maybe a little bit about how this has changed, say, in the last 12 to 24 months?

Rich Pethia: Okay, well let's start with some of the good news. I think certainly we all know that the Internet continues to grow, not just in size — certainly in terms of number of people connected and volume of traffic — but I think the growth is also there in utility, the amount of real government and business operations that are being conducted efficiently over the network. We have new applications being introduced all the time. We have new appliances that allow real mobility. So I think, from the network's perspective, we have a very healthy picture of utility and growth.

User awareness, in terms of the need to attend to security, I think is also increasing. I think a lot more people today, even than just two years ago, are aware of the need to pay attention to security issues. A lot of the Internet service providers are now providing help to their home users with things like firewalls and virus protection software, anti-spyware packages, as well as backup services for important data. So I think that's been a positive change in the industry over the last couple of years.

System developers, providers, I think are all increasing the amount of attention they pay to security and how much money they're spending on trying to do a better job of building security into their products. And while there's still a lot of vulnerabilities found on a regular basis in much of the software that's out there, most of the major vendors now have mature processes in place to deal with these vulnerabilities and get updates out to their customers in a cost-effective and timely way.

And the other trend I've seen is more people are paying attention to security, trying to understand what the security problems are. I think there's increased law enforcement activity in this area. More people are willing to report crimes and get help from law enforcement in prosecuting them, and there's a trend in all the law enforcement organizations to build capability in that area.

Julia Allen: So those are all great measures or indicators that we're actually starting to get some traction on this topic. But I know that the challenges continue to morph and escalate. So what about some of the challenges?

Rich Pethia: Yes, so that's — you're right. That was the good side; now there's the other side of the picture. The bad guys of the world have really grown in level of capability and activity, over the last couple of years especially. The threats have evolved from what we saw years ago — a bunch of zealous amateurs and mischief makers and vandals — to today what's really a very knowledgeable and profit or cause-motivated set of criminals who are using some very sophisticated approaches and building an ever-growing electronic crime infrastructure.

Today, if you want to launch a denial-of-service attack against someone, and you don't have the skill or the desire to go out and build your own botnet, it doesn't matter. You can buy one or even rent one for a period of time. Want to send some spam? There are botnets out there that you can hire to do that for you. If you want to launch a virus that attacks some particular set of organizations, and have one that won't be immediately detected by major anti-virus packages, well there are cyber mercenaries out there today who'll be glad to write that piece of software for you, and give you a money-back guarantee that in fact it won't be detected, at least for some period of time. And if you need to find a way to turn your pirated credit card information or your pirated personal ID information into cash, there are underground markets that you can use to accomplish those goals as well.

So there really is an organized crime activity that's growing and I think it really promises to be a continuing significant threat in the future.

Julia Allen: So if you were in the position of running a major commercial organization or government organization, as a leader what would you feel are some of the key issues that you would need to pay attention to today when trying to conduct a successful business on the Internet, or at least having that as part of your business strategy?

Rich Pethia: One of the things that I still see that troubles me a lot is that a lot of organizations still don't understand the need for comprehensive, continuous security risk management practices. Too often we see organizations that have adopted either a number of point solutions for particular problems, or they've adopted what I call a "check the box practices program" where they know they need to comply to some regulation or another and they put the practices in place just well enough to meet that compliance obligation.

And unfortunately those kind of approaches really provide only limited value because the threats and the vulnerabilities continue to change. So attackers today have a real broad landscape that they can use to attack our systems and when one approach fails, they're very quick to find others. And leaders need to understand that we're facing a dynamic, ever-changing problem, and that their risk-management practices need to account for that.

I think it's also important for them to understand that this is a problem that's not going to go away. The bad guys are becoming more focused; they're more motivated by profit; they're more capable of rendering harm. The changes in the way we use computers, the rise of social networking and the lowering of barriers to privacy, both personal and corporate, can lead to information leakage and exposure.

And certainly we all know about the great increase in mobile computing devices. Today we can walk around with devices that'll easily hold megabytes of data and have them in our pockets. And so we need to ensure that data is protected in these uncontrolled environments, that provisions are made for robust reconstitution in case of failure, and that mobile users have the tools they need to protect themselves (or even self-inflicted damage), which is easy to happen when you're using new technology.

And finally I think there's a need for them to understand and evaluate the risks that are going to be associated with increased outsourcing of IT operations, and with the emerging new computing models that really do make the network the computer. So the computing in the cloud models, the increased move towards outsourcing, means that organizations are going to give up direct control and they need to find ways to deal with that issue as well.

Part 2: CERT’s Evolution: The System Lifecycle

Julia Allen: So how are you positioning CERT to better address the fundamental issues of software and system assurance, in this globally connected world, and help build the trust and confidence that is kind of part of the CERT vision and mission?

Rich Pethia: Well over the last 20 years, one of the things that we've really done is broadened the program considerably. As you know, when we started 20 years ago, we were focused very much on sort of the reactive side of helping people understand how to better deal with problems after they occurred.

But today, our R&D program really now has projects that address security issues across the entire engineering and operations lifecycle. We have projects that answer questions like, “How can we do a better job of building security into complex systems and networks? How can we improve coding practices to reduce the number of vulnerabilities that are released in new pieces of code? How can we more quickly detect latent vulnerabilities in new technologies so they can be removed before they're exploited? How can we better monitor the operation of our systems to detect security problems? And how can we better analyze the masses of security event data that's produced by our security technology so that we actually get actionable information?”

Helping people understand what a complex, comprehensive security program looks like, and having tools and techniques available to them to help them with them with their implementation of those kinds of programs. Helping them understand the threats that we face and the indicators that we can use to detect them. Helping law enforcement organizations deal with this ever growing problem; and with the scale issues that they run into, as computer intrusions now often involve hundreds, if not thousands, of computers and terabytes and terabytes of data that have to be analyzed. So solutions that scale to the problem that we're dealing with.

And finally, very importantly, how do we improve our workforce to ensure that all of our staff members have the skills and the knowledge that they need to deal with their responsibilities with respect to security?

Julia Allen: It seems to me being in this area with the program for a number of years, that the whole complexity — the systems, the systems of systems — not only on the service-providing side, the systems that we're all trying build, but as you said, on the criminal, organized crime, law enforcement side — everything is getting more and more sophisticated and complex. And certainly difficult for one person, or even a group of very smart people, to hold in their heads. Are we kind of trying to break the problem down into parts or looking at it more holistically or maybe a combination of both?

Rich Pethia: Well really a combination of both. Certainly from the enterprise level, with respect to organizations that have to operate computers and provide the products and services that their companies require, they really do need to take a holistic approach. They need to understand the technology. They need to understand security technology. They need to understand the policies and practices they have to have in place in their organization. They need to pay attention to building skills in their workforce so that people don't inadvertently make mistakes that lead to security exposures of one kind or another. And they need to make sure that they do this in a continuous way.

There will be — I don't know what it is — but there will be some major new threat out there six months from now that companies are not having to deal with today but they will six months from now. So the need for constant vigilance and maintaining constant awareness of the threat landscape is important.

At the same time though, to find solutions to these problems, we've got to take sort of a piecemeal approach. One of the things that we've been doing for the last two years especially is working with the law enforcement community to understand some of the issues they have to deal with respect to forensically examining boxes that have been used, either as targets of computer crime, or as devices used to commit crime, and the difficulties they have with dealing with things like full-disk encryption, with the problems that they have now where you can walk into a home computer and suddenly you're faced with terabytes worth of data, And much of the technology they've used in the past simply won't allow the capture of that much information.

So there are those kind of narrow slices where we pay particular attention to important and pervasive problems and try to find point solutions to those things. And at the organization level, help people to understand how to integrate all of that into a comprehensive solution.

Part 3: Broadening CERT's Research Agenda; Working with CERT

Julia Allen: Well you've certainly outlined some areas of interest and thrust and problem spaces that the program's actively working in today. But, of course, research is a big part of I know the program's agenda. So with respect to the program's long-term research agenda, I know that you're reaching out to the broader community, kind of beyond maybe even some of our traditional stakeholders and points of contact to better understand their areas of concern. Can you tell our listeners a little bit about the outreach initiatives that you've put in place?

Rich Pethia: Sure, I'd be glad to. We have a set of people that we work with on a regular basis. Certainly as a federally-funded research and development center, we do a lot of work with the Department of Defense and the Department of Homeland Security. But the problems that they have are not unique to those organizations and very often they adopt technology solutions that have come from some other piece of the world.

So it's important for us to be able to look out across the broad landscape and come to understand what's happening in the entire world of information technology, not just in this country but globally. All government operations, all business operations, have some international component to them, and so we need to look worldwide.

So one of the things we've done is instituted what we call a Distinguished Speaker Seminar Series where we invite people here, to our offices in Pittsburgh, and get them to share with us their perspective and ideas about what the information technology and security issues are. This is something that we've been — had in place now for almost a year and we plan to continue it out into the future. Recently we've been looking into things like control system issues, mobile computing issues, the issues surrounding social computing, and have found them to be areas where there's real pervasive concern and areas where we might need to look in the future about helping deal with particular problems.

Julia Allen: And I know that, as part of our 20th anniversary celebration, you have a big event planned in March of 2009. What's that about?

Rich Pethia: Oh well yes, that's kind of exciting. We're going to have a two-day technical symposium where we're inviting a number of people who have what we think are either very broad or very deep perspectives on security and computing issues in the future; people who can help us understand where the technology is going to go; how they think the use of these networks is going to change over time; what technologies they think are going to be adopted in the future; as well as other people who are coming from a policies perspective, and from a perspective of regulation.

So it's a symposium focused on technical issues of technology, of policy, and of security; and a forward looking event, one that doesn't talk so much about what kinds of things we all have in place today but looks more into the future and tries to anticipate some of the things we'll need in the future.

Julia Allen: Excellent. So as we come to our close, how can business leaders, the various organizations that we interact with, and maybe some that we don't, how can leaders in their organizations best benefit from what CERT is doing?

Rich Pethia: Well I think one of the easiest things they can do is just visit our website. Much of the work that we have is available there: our publications; the podcast series, Julia, that you've put together. Even much of our training material is publicly accessible. And they can also use that as a way to find descriptions of our active projects.

At the SEI, as you know, we have an Affiliates Program where organizations actually send people here to work with us on specific projects. And in addition to that, we frequently set up working relationships with organizations for specific areas of work. So, for example, for the past three years we've been working with a group called the Financial Services Technology Consortium and their member companies, to develop something that we're calling the Resiliency Engineering Framework, which is really a comprehensive security improvement process model that integrates organizations' security and IT management and business continuity practices.

So we have those kind of arrangements that we can put in place for specific projects and it's pretty easy to do. And then finally, the last couple of things I'll just mention quickly, is we do offer a pretty broad set of publicly available training courses from both our Pittsburgh and our DC offices. And we're always open to looking for new ways of working with people who have problems that they think are important, that we think are important, and that would help improve our R&D program.

Julia Allen: Well Rich I so appreciate your making the time today to fill our listeners and our broader community in on your unique perspective on security, the Internet, and all the different things that CERT is doing today, and many of our plans for the future. So thanks so much for your time.

Rich Pethia: Oh you're very welcome. It's been fun.