Building Staff Competence in Security
Transcript

Part 1: Identify and Match Required Competencies to Roles

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. Today I'm very pleased to introduce Barbara Laswell, manager of CERT's Practices, Training and Development Team. Today we'll be discussing how to develop staff competency in security.

So, Barbara, across the security landscape, we regularly hear that people are the source of about 80% of the security problems, and hopefully can provide up to 80% of the security solutions. You know, you always hear "people, process, technology," so we're going to talk about people. So how do we develop people as key contributors to security? What are some of your thoughts about that?

Barbara Laswell: Well, it requires everybody across an entire enterprise to have that as a focus or something that's on their minds in terms of protecting their data and information. And so there are people who in different roles have different responsibilities for the protection of that intellectual capital, or assets for an organization.

And from a system and network administrator/operator perspective, which is the core competence of the area of the program for CERT, we are trying to ensure that there are key skills and competencies that people who are working on critical systems have. So, as a business leader, you have some level of assurance that the staff who is working on those systems are adequately trained to perform those tasks.

Julia Allen: So give me a couple of examples of some of the competencies. Maybe pick a role that's one of your favorites and some of the competencies that you think are really critical and how the efforts of your team help build that competency.

Barbara Laswell: Actually the U.S. federal government has been working on this issue to try to identify across the government, "What are those competencies?" So in the Department of Defense, there is a directive and instruction around training competencies and functional requirement areas in what they call the 8570. But it identifies in good detail exactly what those functional requirements are for individuals who are working on computer network defense systems in critical infrastructure. That would be in a business operation any operational requirements of systems that are running for core business functions, and those people ought to have a level of knowledge and training and experience commensurate with the mission criticality of those systems.

Julia Allen: So I would envision that you'd have certain roles for more senior executives, roles for mid-level managers, roles for technical staff, in terms of what they each need to know? Can you kind of make this a little more tangible for us?

Barbara Laswell: Sure. In a business environment at the manager level on a critical system, they would be identifying the confidentiality, integrity, and availability requirements for that system, and developing policy to ensure that it supported that wherever the data resided in the enterprise. At

Copyright 2006 by Carnegie Mellon University

the technical level, the system and network operator needs to understand exactly what's required to make that happen on a system.

Julia Allen: So they can actually put the practices and controls in place.

Barbara Laswell: Yeah, exactly. And this field, obviously – Internet security – isn't that old, and the challenge for business leaders and critical infrastructures is that the field of knowledge is changing very, very rapidly. And we're having to put in place systems for educating and training people on top of while they're doing all these critical functions.

Julia Allen: Like all this just-in-time training.

Barbara Laswell: Exactly. Just-in-time training, and at the educational levels, educational institutions now have regular degree programs, both at the undergraduate and graduate level, in information assurance and information security. So we're starting to see a maturation of the field itself.

Julia Allen: So because of the undergraduate and graduate curriculum work, you're finding at least maybe fairly recently that they're coming in with a little bit better knowledge and awareness of the field?

Barbara Laswell: Yes. And, again, as a business leader, a hiring manager, if you have a mission critical set of systems, one would want to have a higher level of ability or capability in hiring a person for that level. So you would look, for example, for a degree in information assurance from a center of academic excellence. The Department of Homeland Security and the National Security Agency have identified universities and colleges around the U.S. in almost every state that have these programs that are basically accredited programs for information assurance and information security.

And it's not just on the technical side. It's the policy side as well. So that, for example, we were talking about managers. Again, if somebody is managing a highly critical system, and managing a group of staff in computer network defense, looking for a degree in information assurance from an academic institution in policy in that area would be very beneficial.

Julia Allen: You know, you've tied together some real interesting ideas. You talk about matching the skills and capabilities of staff to the security requirements and the criticality of the assets being protected, the systems and the information and the networks, so that kind of presupposes that as a leader you have some notion of what your critical assets are, and therefore what skills you need to match up.

I mean, maybe for something that's less critical you may not need the same level of skill development, or you can afford to develop the skill as the person matures in the role. So that kind of brings together the notions of risk assessment with competency matching or development.

Barbara Laswell: Absolutely. And so in the early days of this field, everybody needed to know everything. But now that we're able to identify mission criticality and assets in an organization, and then determine risk associated with that, it's those systems that you want to put your most highly trained managers and technical staff on.

And, again, the Department of Defense has recognized that, so in the computer network defense service provider area of work which has the most mission critical systems for the Department of Defense, those are the ones that require the most level of skill. So, again, in a business enterprise,

Copyright 2006 by Carnegie Mellon University

those mission critical systems, services, functions, information – that's where you would want to put your energy in having somebody that's highly trained. But there's no reason to have that across all of the systems.

Julia Allen: Well sure, that's like we say, "You can't secure everything," so you kind of want to be selective about where you put your greatest talent.

Barbara Laswell: Sure. But it's important at the enterprise level for all of the employees, all staff, to understand confidentiality, integrity, availability as principles.

Julia Allen: So there is the fundamentals.

Barbara Laswell: Exactly. When they're generating, creating data, knowledge, information, they have a fundamental understanding of how to begin to protect that from the very beginning. So we talk about building those protection strategies in at the very beginning of the life cycle of creation of product development, new service development, software development. That assurance level needs to be thought of at the very beginning.

So if we build a culture of security in our environment, whatever our business enterprise is, if we have everybody thinking along those lines from the beginning, then it isn't as difficult later on to hardwire on security or to determine later on that this is really a highly critical information asset, and it hasn't been structured.

Julia Allen: Right. So you're trying to deal with it after the fact, which is always more costly and not as sustainable a solution.

Part 2: What Skills Should a Hiring Manager Look For?

Julia Allen: So let's shift gears a little bit. I mean, you're obviously a hiring manager. You look at people often, both for your own team and as you're helping to educate and train your customers and your clients. If you're hiring someone for, let's say, a particularly critical set of assets, or a system or a sub-network, what kinds of skills do you look for as a hiring manager?

Barbara Laswell: Well, fortunately, again, the field is maturing so that there are certifications out there that give a level of assurance to a hiring manager that the person has acquired a baseline set of skills in information assurance or information security. So, on a critical system – that would be the first step, looking for somebody who carries some certification in information assurance.

Julia Allen: Okay. Are there certifications that you're able to mention or recommend that you look for or you think are particularly reputable?

Barbara Laswell: I wouldn't recommend them, but I can say that the Department of Defense has a list of certifications that meet those standards for functional requirements in information assurance positions, which actually works for business enterprises as well. It's really not just a function of the Department of Defense. And so they're all listed. CISSP exam is an example of one that's generally accepted.

Julia Allen: The CISSP exam from the –

Barbara Laswell: ISC^2, as a generally accepted, broad understanding. The body of knowledge is fairly broad. Depending on what the level of technical competence or managerial competence in IA

Copyright 2006 by Carnegie Mellon University

one needs, that's the level of certification. Actually the cert.org website lists links to those certifications through those documents in the 8570.

Julia Allen: Right. We have some of those references in the show notes, so that will give folks a chance to take a look and see what makes sense for them.

So let's say that you've got staff in-house. You either have acquired new systems, or a new customer, or a new client. Your security requirements are becoming more complex and more robust. What have you seen are effective approaches for training in-house staff, people that you already have and you want to develop their skill further? Is anything different from what you've already said?

Barbara Laswell: Yes. There is something different. One of the challenges about information assurance and Internet security is the rapidity with which information changes. This is a field that's highly in flux in terms of the knowledge base. So it's very important that there's a continual learning development cycle for especially critical function staff.

Julia Allen: So what you're saying is that's probably part of the cultural norm that people understand that part of their job is to stay current.

Barbara Laswell: Absolutely. And that, in a global, distributed enterprise, is a challenge. The model of sending people to training away from their work for a certain period of time doesn't work too well in information assurance, because first of all, we're in an environment where there's a shortage of supply of people with the right skill sets. And then they're working on critical systems or critical areas, so there isn't a lot of time for them to be away from their jobs to acquire the latest skills. And so it's very important to have scalable, globally distributed, asynchronous methods for their acquiring those knowledges and skills.

Julia Allen: So computer-based training or web-based training, or information that they can go to when they need it?

Barbara Laswell: Absolutely. Just-in-time learning for just-in-time application of a skill. So at CERT, we've worked on this problem and we have the Virtual Training Environment available to anybody, anywhere, anytime, around the world, at the module level of topics in information assurance. There's lectures and demos and virtual environments for practicing skills at the individual level.

So it's very important that the baseline sets of skills that people bring to with certifications are kept current. Then in addition to that, in addition to individuals, people need to practice together in teams, in sort of live-fire environments.

Julia Allen: Right. This is a team sport, right?

Barbara Laswell: Exactly. This is a team sport, and so we're also working on ways to have that happen again asynchronously, virtually, anywhere in the world, because most of us are connected globally to some partner or a part of our organization itself. So we're looking for those, you know, Internet-based, scalable training solutions for acquiring the right knowledge and skill sets for individuals *when they need it*, because there's so much information to learn and it changes so rapidly that it's important that people have that just-in-time access.

Julia Allen: And for some of this, in your Virtual Training Environment or in some of the other distributed, asynchronous environments that you've seen, do I understand correctly that they're

Copyright 2006 by Carnegie Mellon University

also exercise-based, where they can actually get into labs or exercises and actually try out different approaches?

Barbara Laswell: Absolutely. We don't want staff trying on production systems their newest skill.

Julia Allen: Right. Not a good idea.

Barbara Laswell: So we've worked very hard to create virtual, very complex, networked virtual environments that people can do what-if scenarios in — scenario-based environments that really mimic the environments that they're in. And apply skills. Have things break. Reset.

Julia Allen: They have to rebuild or restore a system that's been compromised.

Barbara Laswell: Right. And in these training environments that we're building, the sandbox environments, you're able to introduce the latest intruder attack. A certain network operator may never see this come across the system, or they may, but you don't want them to see it for the first time in a live production environment.

One of the advantages of having exercise environments, lab environments, in the Virtual Training Environment is that they can see this activity or trends or patterns of intruder behavior or compromises to systems without experiencing them for the first time on a critical system.

Julia Allen: I'm kind of reminded in the research and reading I've been doing about business continuity, and business continuity planning, business continuity exercises, which are obviously much broader in scope in some cases than information or computer security. But the same notion of exercise, exercise, practice, practice, so that when the real thing comes down the road, you're much better prepared, and it's not as much of a panic or a reactive situation.

Barbara Laswell: Absolutely. And we want people practicing together in teams, not as individuals. They can learn and acquire the base-level skills as individuals, but they need to be practicing in these environments in teams.

Julia Allen: Yeah. As a perfect example, with your incident management work so much of what happens has to do with communicating with the right people, interfacing properly with the press, interfacing with law enforcement. Just all those different interactions clearly call for some team interaction in advance of having to actually deal with the situation.

Part 3: Creating a Culture of Security; Actions Leaders Can Take

Julia Allen: To kind of take us to the close of our conversation, you had touched on earlier about this notion of a culture of security, kind of an elusive concept to get your head around. For example, if I walked into an organization I would say to myself, you know, "How do I know if this organization has a culture of security?"

So from a staff competency and staff development perspective, can you say a little bit about what you consider that to be, and how a business leader might go about helping build such a culture, again, from a staff development point of view?

Barbara Laswell: I think it's really important that people understand that information or data that's created or used or transmitted, that there's confidentiality, integrity, and availability. That that information, and each piece of that information, needs to be protected in some way, that if it's private or confidential, or there's a business reason.

Copyright 2006 by Carnegie Mellon University

In our complex environments, they're all mixed together. I mean, there's personal information. There's business information. It's not easy if you're trying to after-the-fact if you're tagging it. If people can understand that from the very beginning, it helps.

Julia Allen: So you need to have some kind of a notion of how you're going to classify or structure or categorize all the different types of information that you have.

Barbara Laswell: If we can bring a risk-based approach to each person, no matter what level they're working on in the organization. So this piece of information that I'm working with, if it were modified in such a way, what impact would it have on my customer? What impact would it have on another business service within the organization? What impact would it have on a partner?

Julia Allen: So you're saying, "Have that kind of thinking."

Barbara Laswell: Thinking from day one. That's the culture: that everybody thinks that way from the very beginning. And then availability – what happens if this isn't available? Can I live with not having this information available for X period of time? Well, no, not across the board. But for this particular customer, it must always be available. But that's only a certain portion. I can live with the risk of the rest of it.

So I think that we've delegated that authority to mid-level managers or managers, but we all, in an information-based society, within an enterprise, every person needs to understand that they're developing intellectual capital for that enterprise, and you can't have just the risk manager worrying about that. It has to be considered from the very beginning.

And you were talking about internally within organizations, but I think obviously with partners and outsourcing, it's very important to write into all of the outsourcing agreements certification requirements for staff that are going to be working on certain systems as partners.

Julia Allen: Great point.

Barbara Laswell: And so you can write that actually into the service level agreements that the competencies be clearly identified, and there'd be training plans in place for outsourced staff.

Julia Allen: So those are great steps if I want to put that in place, either in my organization or in a partner organization, great steps to say, okay, make that explicit. Make sure people understand what standards you're holding them to, what policies and practices they need to adopt. But then I would obviously assume there has to be some kind of a demonstration, you know, a monitoring and a review and an enforcement aspect to make sure that that's actually happening.

Barbara Laswell: Right.

Julia Allen: So are there other resources that you'd like to point out to us? You've pointed out several which are described in the show notes, but other resources from your team, from your curriculum development activities that you'd like to highlight, or have we pretty much covered that?

Barbara Laswell: Well, I think the one thing I didn't mention was the Committee on National System Security, CNSS, has role-based functional requirements for specific positions, so information systems security officer, information systems security manager. And there are five or six different training standards and competencies for each one of those roles. They're explicit, such that you could use them in a hiring interview. You go to password-protected systems, for example. How

Copyright 2006 by Carnegie Mellon University

would you do this? How would you do that? At the manager level, what would be the policy that you would want to ensure would be in place to enforce this standard?

And so those standards, as well as the ones that are in the DOD for the 8570 training standards, present a nice base that we can work off as a whole field of business and information assurance professionals develop, and we can begin to demand that of people that we're hiring. Demand that as part of a development plan for our staff. Demand that for our outsourced providers. Demand that of our partners.

Julia Allen: Yeah. Because up to this point it's been fairly recent that we've had that kind of more precise and more detailed specification of what it really takes to successfully execute some of these roles. So having that, as you say, kind of something that we can use across the board could really help elevate the whole practice of information assurance in our community.

Well, I really very much appreciate your time today, and really actually benefited quite a bit from some of your comments and remarks. And I look forward to talking with you again.

Barbara Laswell: Thank you.

Julia Allen: You're welcome.

Copyright 2006 by Carnegie Mellon University