A New Look at the Business of IT Education
Transcript

Part 1: Filling a Gap

Stephanie Losi: 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 Stephanie Losi. I am a journalist and graduate student at Carnegie Mellon, working with the CERT Program. I am pleased to introduce Larry Rogers, a senior member of the technical staff at CERT and Chief Architect of the Survivability and Information Assurance Curriculum. Today we'll be discussing the SIA Curriculum. So, Larry, I guess I just want to jump in and start by asking you what prompted you to start developing the curriculum.

Larry Rogers: The Survivability and Information Assurance Curriculum became obvious to me as a necessity because I was seeing that there were too many system administrators who had been trained technically in how to operate the technology but really didn't understand what they were doing. If the technology didn't work as it was expected or there was a new generation of technology, frequently I would see an administrator being lost and not knowing what to do. And so I felt there was a gap area there that we could address through some education, some real-world situations that we'd put the system administrator in and would really help system administrators know better what they were doing and make them more resilient to changes in technology or technology not operating correctly. So that was the basis for doing the curriculum.

Stephanie Losi: Okay, so it sounds like you sort of aimed for something that would teach people how to adapt.

Larry Rogers: That's exactly the case. Technology changes frequently, technology doesn't always work correctly, and the people who are able to do the best in their jobs are the ones that can react to those changes or unusual situations.

Stephanie Losi: Okay, so can you talk a little bit about your approach to technology education in general? What do you think is most often missed, and how did the SIA Curriculum attempt to fill that gap?

Larry Rogers: The first course in the curriculum is really the basis for it, which defines, stresses, and shows examples of ten principles of survivability and information assurance. It's intended to be independent of technology, or applicable to any technology to varying degrees. And so the idea is that system administrators learn those principles, and then the remaining two courses in the current version of the curriculum apply those principles to networking and then to an enterprise network.

Stephanie Losi: Okay, so can you tell me what kinds of students are most likely to benefit from this curriculum? Let's say I'm a manager. How can I sort of tell, well, who might be a good candidate for this course? Who would I want to send to get the most out of the course?

Larry Rogers: The curriculum is designed for experienced system and network administrators. Another key aspect of students who are successful in this are students who want to know more,

who desire to learn what's going on, and simply are not interested in just stopping at operating the technology. They may be people who may be managers in the future. In some cases I'm sure businesses look at people and say, "Oh, this person has a managerial future, and I'm going to push them in that direction." These are people who can think out of the box in today's environment, who are interested in learning more, who are interested in doing more, but who also have a business sense.

I think it's very much the case that system administrators can operate the technology, can make the technology dance to any tune that they choose, but don't necessarily connect the technology to the fact that the business has a mission, that the business has risk as part of its way for operating, has policies and procedures and governance, and the system administrators that recognize that the technology has to fit into the business and complement the business rather than drive the business are the ones who are going to be the most successful.

Part 2: Curriculum Fundamentals and Goals

Stephanie Losi: And so what will the system administrator find when he or she attends the course?

Larry Rogers: Well, they'll encounter things that they're probably not used to. In most cases, they would be taught technology, but in addition the SIA Curriculum is also going to teach things like communication skills. For example, there was an advertisement on TV three or four years ago where the system administrators had just upgraded the systems to the next version, and it was the end of the week and they were having a party, and the manager came down and said, you know, "Why are you partying?" And the administrator said, "Oh, we just did this technical thing." The manager's eyes glazed over, and then the system administrator said, "Oh, because of what we did we're saving five cents per transaction," and then in the last scene in the commercial all of the system administrators and the managers are partying together.

The key to that scene is that the system administrator was able to communicate to the manager in the language that the manager understood and could deal with and process, and I think that's very important for system administrators. That's one of the ten principles, is communications. And the idea behind that is it is no longer the case that the system administrator is the unkempt person in the back room who people don't talk to, but it is now the case the most successful system administrators will be the ones who can speak in the language of many different people within the organization, can understand business mission, can understand the way businesses run, and can live within the constraints of policies, procedures, and governance. That's what's most important these days.

So the students who are able to adapt will be the ones who will be able to deal in that environment, and those are the kinds of things they'll see in the SIA Curriculum. They are put in that position. They talk to the instructor as though they're the manager. They have a policy and procedure manual that's part of the course that they have to live within the constraints of. They have a risk analysis to help guide them in what they're doing in their tasks. All of these I believe are intended to make the SIA Curriculum be practical and appropriately constrained, and the students live within those constraints.

Stephanie Losi: Could you talk a little bit about some more of the other principles underlying the course?

Larry Rogers: The key principle—there are ten principles. The first principle is the principle of survivability, and that tells the system administrator not to concentrate necessarily on a specific computer system being up all the time, but rather the business mission surviving in the face of

attacks, breakdowns, user errors, and such. Going back to the first World Trade Center attacks in 1993, there were some number of those companies in the lower floors of the World Trade Center who, when the bombs went off, simply walked up to midtown Manhattan and continued their IT operation. The IT operations survived those attacks even though some specific computer systems no longer worked. There were some other businesses that simply went out of business that day. They were not survivable at all. We know about survivability. We don't send one single soldier to fight a battle. We send multiple soldiers, we send multiple warships, we send multiple planes into a battle so that we can achieve the mission that we're trying to achieve. The same is also true with computer systems. You may have redundancy—if something breaks or is not operational for some reason, there's a backup so that you can still continue to achieve the mission.

Stephanie Losi: So what you're really doing, I mean, you're tying these well-known business concepts into IT with these principles.

Larry Rogers: Yes, that's exactly the case, and I think it's all too often the case that the system administrators may not even know what the mission of a business is. They may simply know, "I have these computer systems that I have to deal with, I can make them do these things. Oh, by the way, what is it that we sell again?" and have lost contact, lost the connection between the physical hardware sitting in the machine room and the mission of the business. So survivability is the number one principle.

The second principle talks about the fact that everything in a computer is data. Normally, we think about data as being a file created by an application. That of course is data, but also the application is data. It's a collection of bits that live on a disk that are accessed in some fashion, and the operating system is also data. All of these things are data, and when you deal with data and securing data, one of the things you're trying to deal with is called confidentiality, where you want to keep things away from people. For a piece of paper, you may put it in a file cabinet, lock the file cabinet, lock it in a room, lock it in a facility where there's a guard, so you're using multiple layers of security. In the case where you can't keep people away from the information, you use encryption, and the strength of the encryption depends upon the lifetime of the data. For example, if it took two years to break an encryption of an Internet transaction, and at the end of that two years you were able to extract a credit card number, what are the chances that that credit card number would still be valid? Probably pretty good, so if in fact you can break the transaction, then that encryption is not strong enough to guard the data through its lifetime.

So the idea is to recognize that everything is data. The big three attributes of data that you're concerned with are the CIA: confidentiality; integrity, which is, has this data changed in the way that I'm not expecting it, and can I recognize it then?; and finally availability, can the people who need to get to the data get to the data whenever they want to get to it, within whatever the constraints are, twenty minutes, two hours, whatever?

The third principle says that even though everything is data within the company, not all of that data has the same value. And so it's important to recognize the most important data with respect to the mission of the business and put the most amount of safeguards on that, rather than saying, "I'm going to apply all of the safeguards to all of the data." There simply isn't enough time anymore to do everything everywhere. So a system administrator has to be intelligent in where they apply safeguards.

So those are the first three principles, to highlight those.

Stephanie Losi: What I'm hearing you say is that basically the conception of a system administrator has changed, from this person who is very, very knowledgeable about technology but maybe not

so much about the rest of the business, to someone who is sort of tied in to the business mission directly. Now how does that evolution work?

Larry Rogers: The system administrator needs to be sensitized to the fact that there is a business, which is a relatively new concept. It used to be the case that the system administrator was the king or the queen of the domain, and whatever they did was how the business worked. Now that situation is completely opposite, where the business is king or queen and the technology is really an asset. Technology is like a pencil. We don't think about a pencil, we simply use a pencil. There are some people who are concerned about the technology of the pencil—what it takes to make, what it takes to sharpen, is the lead too hard, is the lead too soft, can the eraser erase the pencil—but fundamentally we don't think about that. We simply do whatever we need to do with the pencil. And at this point in time and in the future, it is my opinion that computers are going to be thought of that way. They are simply going to be an enabler of business. Yes, there will be a collection of people who are really concerned about how the technology works, but that's not the part that drives the business.

Stephanie Losi: Right, that's behind the scenes.

Larry Rogers: Right.

Stephanie Losi: So by fostering this rapport between managers and the IT staff, by kind of getting the IT staff to think about the business mission and by having the managers sort of understand where the IT staff are coming from, how do you think the material learned in the SIA Curriculum can carry over to the business environment when students who have taken the course return to work?

Larry Rogers: They should be in a position where they have more knowledge about business, which I think is a non-traditional discipline for system administrators to think about, and in fact what I believe we're beginning to recognize is some of the best administrators these days are the administrators who were taught out of a business school. We traditionally have thought that the best system administrators might be the computer scientists who may have more savvy in software, or computer engineers who may have a mixture of hardware and software expertise. We've thought of them traditionally as the best administrators. These days our thinking has changed to say that these administrators need the business sense.

So as the SIA Curriculum has been out and around, we're finding and talking to a lot of business schools and business departments to say, "This is a curriculum that you can use to augment what you're currently teaching." Still leaving the computer scientists to make applications, to computer engineering schools to make hardware miniaturized, make new features faster, smaller, cheaper, but recognizing that the better administrators actually come out of the business schools.

Part 3: Evolving and Gaining Buy-In

Stephanie Losi: So what were some of the challenges that arose while you were developing this curriculum, and how did you approach those challenges?

Larry Rogers: I think the biggest challenge was the fact that this is a new direction for administrators. Administrators even in graduate schools who we've talked to, some of the students in those schools want technology. The businesses want them to have technology, therefore schools teach them technology. So I think the challenge has been to say those are important skills, because at the end of the day some system administrator has to sit at some keyboard or address some display with a mouse and control the technology to do what they want it to do.

Stephanie Losi: Right, they have to type in commands.

Larry Rogers: They have to type in commands, but the question then becomes: Are those commands doing what's necessary to support the mission within the constraints of the business, within the practical risk analysis parts of the business and such. Can the administrators do that? So the challenge has been to say, "Everything that you've learned is important, but it's not enough, you need to know things in these other areas," and to get faculty to buy in to the concept, to get students to say, "This is new, I really need to learn these things," and to engineer courseware that supports that—puts students in situations.

A key example is in the third course. The third course is basically a culmination of all of the curriculum, and in the third course the students are put in the position of being a new system administrator hired into an existing enterprise with an existing network. All too often I think we teach system administrators how to build a brand-new network from scratch. That's how we teach them, but I think that's not the more common situation that a student finds themselves in. Instead, the third course says, "You're brand new, you have a network, the network is documented in some fashion, good, bad, or indifferent, there's a collection of computer systems in there, how do they interoperate, what's out there, what's the inventory?" Perhaps some of the computer systems have already been broken in, and in the process of understanding what's on those computer systems you may see signs of intrusions. The students are also put in the position where they have to make whatever changes the exercises require of them within the constraints of policy and procedure, keeping in mind the business mission, keeping in mind that there is risk analysis, and juggle all of these as well as talking with the instructor as their manager or as other people within the organization and trying to say, "This is what we're doing, this is why we're doing it, this is why it makes business sense."

That, I believe, is a more practical approach to how administrators should be taught. In addition, they do need to know the technology. There's no substitute for understanding the technology.

Stephanie Losi: Right, so what you're saying is—just to go back to this very briefly—the ideal student would have the technical underpinnings, would come in, and this is sort of to teach them the business sense, how do you apply it to the business.

Larry Rogers: The key word is complementary. The SIA Curriculum is complementary of technology training. I could see, for example, a student getting a certificate in SIA—that's not something that currently exists, but I can envision that framework—complementing any certificate they have from Microsoft, from Red Hat with Linux, from whatever other certificates are out for technical training saying, "I understand SIA and what those educational underpinnings are, and I can apply those in a Microsoft environment." And it's the combination of those two that I envision to be a super certificate.

Stephanie Losi: All right, and just to close up here, how would you say working on the SIA Curriculum has shaped or informed your overall view of technology education?

Larry Rogers: Technology education is still very important. You still have to interact with technology. But what's it's done is to extend my thinking to say that technology exists for a reason. And so now I'm looking at a lot of the areas that I have traditionally worked in with respect to their impact on the business, and saying, "System administrators need to know the business, it's not just enough to know technology. Technology is important, but by itself it's not sufficient."

So I've learned to at least say, "What's the impact on business, what are the metrics of performance, what does this cost, what's the benefit, are we avoiding costs, are we reducing costs?" Really, the business component of running computer systems has been my greatest growth over the four years I've been working on this.

Stephanie Losi: All right, thank you very much. This has been great, I have learned a lot, and I've enjoyed having you here.

Larry Rogers: Thank you.