What Business Leaders Can Expect from Security Degree Programs
Transcript

Part 1: Nuts and Bolts versus the Big Picture

Stephanie Losi: 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 Stephanie Losi. I am a journalist and Carnegie Mellon graduate working with the CERT Program.

Today I'm pleased to introduce Sean Beggs, Director of the MSISPM – that's Master of Science in Information Security Policy and Management – Program at Carnegie Mellon. In the interest of full disclosure, I attended this program and graduated in May 2007. Today, Sean and I will be discussing what business leaders can expect from students who are hired out of various types of academic information security programs, so, Sean, welcome.

Sean Beggs: Thank you, Stephanie.

Stephanie Losi: I'd like to start by asking what, in your opinion, are the most important skills a student in an information security program can acquire?

Sean Beggs: Well, I think the most important skills a student can learn is the process by which they attack information security problems. By process I mean the underlying factors found within, around, or resulting from information security issues. Having the ability to see the big picture, in addition to understanding the messy details, as the transferable skills that the students need to acquire early on.

Stephanie Losi: Okay, so it's not so much, you know, "Configure this router," as "Understand the whole picture"?

Sean Beggs: That's right. I don't think having a certain specialty in something like configuring a router solves all of your problems that you see in the field.

Stephanie Losi: All right, and do you think that the skill set that you think is important really differs between graduate and undergraduate programs?

Sean Beggs: Yes, I think to some degree. The undergrad programs generally focus on building the skills within the foundations of a program of study. Graduate programs, like ours, the MSISPM Program, we try and take it to the next level and develop the skills needed to succeed as a senior security professional.

Stephanie Losi: All right, and how would you say the backgrounds of the students affect that? What are you really trying to give people as a base, considering that they may come from a variety of backgrounds?

Sean Beggs: I think what we try to achieve is give all of our students a balance, because certain students come from various backgrounds and their strengths coming in vary. But with our program,

we reach across those disciplinary lines and so that we can take someone who is technology savvy in terms of routers, like you mentioned a few minutes ago, we can take that person and make them appreciate the other aspects of information security. And, along the same lines, we can take someone else who doesn't have a clue what a router is, except for something that flashes in their home office so that they can get wireless connections, and make them understand and appreciate what a router is capable of defending from a security standpoint.

And our goal is basically to train our graduates so that they see how to bridge the disciplines of information assurance. Our grads can oversee the security life cycle, including planning, acquisition, development, and evolution of security infrastructures. And, to me, that's the well-balanced, well-structured approach to giving someone the tools and the knowledge to tackle those security issues.

Stephanie Losi: And so how do you think that employers might see skill sets differing among graduates of various types of information security programs and specifically speaking from your experience as well?

Sean Beggs: The skills that I've seen — the school of thought, I should say, that I've seen — includes ones where they believe that the nuts and bolts of security practices will win the war of information security, like the routers and firewalls and network security appliances. If you put those in place, you're good to go. But on the other hand, you have the schools of thought that believe we need to just regulate everything with policy and if people realize the consequences due to policy it'll stop the bad guys.

But my belief is that the most compelling area to develop is where those intersections meet, right? So the areas where the nuts and bolts meet the end user, and if you can identify and manage the advancements in technology while taking into consideration policies that impact the end user, all of those need to be utilized so that all stakeholders in a particular organization, and the technology in that organization, is leveraged in such a way that you cover all of your bases and kind of back to that balanced approach.

Part 2: How To Help Ensure Graduates Are Successful

Stephanie Losi: All right, so let's look at this from a business leader perspective for a minute. I know that in a discipline like information security there is not, for example, a *US News & World Report* ranking that says, "Well, these are the top 50 information security programs." So how can a business leader look online or look in a magazine? Where can they look to locate programs that are teaching the kinds of skills they want to bring into their organizations?

Sean Beggs: Well, the National Security Agency standards for Academic Excellence in Information Assurance is a great starting point, I believe.

Stephanie Losi: Let's flip this around a little bit, what do you think information security students are looking for in an employer?

Sean Beggs: Well, generally aside from a terrific salary, right?

Stephanie Losi: Right, everybody is different, yeah, but yes, generally.

Sean Beggs: Generally, I see that our students are looking for support from an employer standpoint. Our students want to have an employer that's going to engage them, not only in their

goals, their day-to-day goals and assignments, but is also going to challenge them to go out and learn more through certification or through going to security conferences and whatnot.

So I believe that the students want to see an active investment taken by employers, and from my standpoint employers — it's a great opportunity for employers to take advantage of hungry new hires who want to get out there and continue learning and be the best professional – security professional — that they can be.

Stephanie Losi: And from the employer perspective, what do you think are good questions that interviewers can ask students to gauge their level of knowledge and preparedness for the real work information security work?

Sean Beggs: I think that organizations are different, across the board, so it's really hard to identify exactly how one organization selects an employee versus another based upon a question or two. But I think the key where organizations would probably benefit — I think that the organization has to try and spend some time to ask how a student thinks about information security and how he or she mentally calculates and identifies all of the angles of information security. Because that said, you get an idea of what the person, what the individual is like and how they're going to go about tackling an ever-changing landscape, and certainly information security is changing from day to day.

Stephanie Losi: Right, I mean because it's relatively easy to look at a course listing and say, "Okay, well, you know, these students should know XYZ," but how can they really tell? You know, how do they dig that out? So I think that's a good suggestion, to kind of try to look at, well, how do people think?

Sean Beggs: I don't want to suggest that we need to take out a psychological assessment of a student or a potential employee, but I do think it would help organizations to understand exactly how they're going to approach these problems and what they think about problems that deal directly with information security. We already know they're bright. We already know they've been through the rigors of academic professions, so we know that they have an undergrad degree and in many cases a master's degree, so these are bright individuals. But, again, to make certain that you get the right fit, the person that's going to fit into an organization and a person who's going to do well and succeed in that organization based upon the business of that organization, you need to think about what your potential employee is going to think about information security.

Sean Beggs: Does that make sense?

Stephanie Losi: It does.

Sean Beggs: Okay.

Stephanie Losi: And then going on from that, what can organizations do, do you think, to ensure that graduates of information security programs have a smooth transition from academia into the work world?

Sean Beggs: I think an organization should provide a graduate kind of a working tool, almost a 100-day plan, because it can be kind of a hard transition. But if the organization provides the student, I have a hard time here, I'm saying student but I mean new employee.

Stephanie Losi: New graduate, right, new employee.

Sean Beggs: New employee, if they provide him with a 100-day plan that clearly defines their expectations of the person, the chains of command, how things get done around the organization, and how all associates fit together within the organization to meet the goals, I believe that that gives that person the best tool to succeed and to get off to a running start.

Stephanie Losi: So what would you say is really the advantage of hiring a graduate of an information security program specifically, as opposed to, for example, a computer science grad who is self-taught in security? I mean, like what would you say? Is it a stamp of approval from the program? Is it, you know, the knowledge that they've taken XYZ classes? Is there a specific skill set? What do you think that is?

Sean Beggs: Well, I think it's a little bit of both, or all three that you just mentioned. If you take someone who is self-taught — and believe me there are some bright individuals out there who are self-taught and do very well and are very important to where they're working — but in some ways you can't measure what they're taught in, right? So when you take someone who has an actual degree, there are measurements and standards that person has achieved. And for organizations who want to perhaps market that to their end users, to their customers, it's a huge advantage.

And, plus, you know, let's face it, when people go on to secondary education and, they undertake graduate studies, they're not messing around. I mean these people are living and breathing in this environment, whatever that degree program might be. And that, again, states I believe a certain amount of commitment that that individual has for a certain discipline like information security.

Part 3: Keeping Pace as the Security Field Evolves

Stephanie Losi: Okay, and how do you personally think that the field of information security will evolve, and how will that affect in general educational programs geared toward it?

Sean Beggs: Well, there are a couple of ways of looking at this. Maybe information security takes on a life of its own, meaning that we come to the point where everything can be taught, all the foundations can be covered of what the right policies are, what the right technology requirements are, how to train users. And we come to the point where we're almost so aware of it that it becomes second nature to everyone, right? It's how do you pick up a telephone and dial the number kind of deal? It just happens.

I don't think that will happen, though. I think you're always going to have issues, and every generation that comes to play within those issues and that's impacted by those issues will need to be trained. And to some degree I think that that is going to be the cycle that continues no matter what. Sure, we might have different issues, meaning, you know, we now have a secure internet protocol that we can all get online with, but after that you still have the operating systems. You still have the problems that crop up when pieces of software are loaded, and you still have people who just want to see, "Hey, can I break this? Can I beat the system?" And you're still going to always need folks to think about those issues and to defend against those issues.

Stephanie Losi: So at a certain point, do you think there is too much for any one person to know, and do you sort of see specialization happening down the line, or do you just see sort of an evolution toward an understanding at perhaps a higher level because the lower-level stuff is taken care of? How do you think that will go?

Sean Beggs: I'd like to say that we'll see specializations crop up. I like to say that only because it seems to me that if you specialize, you can certainly concentrate your efforts in areas and you can train individuals within those areas. But it's really hard to say what changes are going to come at

us. What's going to happen if we see a complete shift in the way people utilize computers and utilize networks? It's really hard to say where it's going to go.

It will be interesting to see which way, which direction it takes. But in many ways the direction is shaped by the people we train today.

Stephanie Losi: All right. And so what do you think about — how do you decide what you're going to teach people in an academic program? I mean, what is the process by which you do that?

Sean Beggs: Well, I think that what drives the business of education has a lot to do with the institution that's offering that education, right? So research institutions versus for-profit institutions have very different goals and objectives in mind. And we need to understand, from the standpoint of where our grads go, what skills do they need so that when they get to the organization and they've gone through their 100-day plan with the organization that they can then hit the ground running with the skills that we've taught. So I think it's a combination of meeting the institutional organization's objectives, figuring out where our grads go, and then finally what our grads are going to be doing with the organizations who hire them.

And that constant review of those three aspects help direct how our education is planned and what courses are offered and why a particular course is now in the limelight and why something else is not.

Stephanie Losi: Is there a process by which business leaders in organizations can provide feedback back to educational institutions to say, "These are the skills that we need"? Do you think that's going on right now and, if not, I mean, are there ways that this could be facilitated?

Sean Beggs: I think in our organization it does goes on maybe informally. I would like to think of a more formal process that could be put together, maybe some sort of program where these initiatives are reviewed every year or two. On a national level, that would be great, but in practice I don't see that happening anytime soon.

Stephanie Losi: Okay. And where can our listeners learn more about this?

Sean Beggs: Well, obviously the SEI website is probably the best place to start, CMU's website as well. If you want to know more about our program, MSISPM, it's www.ism.cmu.edu, and I welcome email to my address. It's sbeggs@cmu.edu.

Stephanie Losi: All right, well thank you very much Sean.

Sean Beggs: Thank you, and I enjoy seeing you again now that you're a grad. I should mention too, in closing, that these comments are strictly my own. They don't reflect our faculty members or the administration of the Heinz School or the MSISPM programs.

Stephanie Losi: All right, thank you very much.

Sean Beggs: Thank you.