How to Become a Cyber Warrior
Transcript

Part 1: Growing Demand for Skilled Professionals; Startup Resources for Getting Smarter

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 our podcast website.

My name is Julia Allen. I'm a principal researcher at CERT, working on operational resilience and software assurance.

Today I'm pleased to welcome Dennis Allen. Dennis is one of my colleagues at CERT. He's a member of CERT's Workforce Development Team.

And today he and I will be kicking around some ideas, and some resources, about what it takes to become a capable cyber warrior. This is a skill that is in increasing demand and very short supply.

So with no further ado, welcome Dennis. Glad to have you with us today.

Dennis Allen: Thanks. Glad to be here.

Julia Allen: Okay. So let's get some terms and ideas, some foundational work laid. So when you talk about cyber warriors, what do you mean? What is a cyber warrior and why is the demand for folks with this skill set growing so much today?

Dennis Allen: Well first of all, 'cyber' in today's context really means computer. It's just that cyber's way more cool and exciting. So it's become quite popular to use 'cyber.' So when you hear 'cyber warrior' or 'cybersecurity,' it really can be translated to computer warrior, computer security. It's just way cooler to use the word 'cyber' I guess.

Julia Allen: Right. It seems to have a lot of cachet. Right?

Dennis Allen: Absolutely, absolutely. And so when we're looking at a cyber warrior, it's really your traditional information technology, your information security professional that's responsible for computer network operations. Those computer network operations might be computer network attack or defend or even computer network exploitation.

Many of today's government, military, and private networks are connected to the internet or each other.This is necessary for access and functionality. But what it does do is it opens up a pathway for criminals, for foreign militaries, for other bad guys. And then this pathway can be used to compromise critical infrastructure or information.

So the big need for the United States now is to develop new cyber warriors. These cyber warriors have to be able to defend these critical systems and these pathways. They have to be able to, in some cases, perform offensive operations.

Julia Allen: So is it fair to say that just like in normal day-to-day life we have crime of all types and people with ill-intent. And so it's not surprising that that kind of behavior is showing up on the internet, right?

Dennis Allen: Absolutely. As we become more dependent on computer systems--and they're so prevalent for our day-to-day work, and so much of it's being used for commerce and for business-- they naturally become bigger targets for the bad guys to try to get financial gain or intellectual property; the types of assets that we hold valuable.

Julia Allen: Excellent. Well thank you for that introduction. Okay, so here I am, I'm a student maybe in high school, maybe in college, or maybe I'm a professional who's looking to make a career change. So how can I get started or get a little smarter about security threats and some of the basics, to make a determination if this is a field I'm interested in?

Dennis Allen: That's a great question because I actually get that one all the time. And you get it from varying levels of expertise. You might have a business leader that has that question. I might get it from my brother that's taken one computer class. You might get it from somebody that has no idea of anything at all about computers.

So there's a number of resources that you can access -- a number of websites, videos, tutorials and things that you can go to, to explain what some of the common threats are, or they promote online safety. And that's really a good place to start because that gives you an idea of what some of the bad guys are using, the tools and techniques that they're using, to try to compromise your systems and your information.

So once you better understand those types of things, then you can start to learn about the technologies that you need to have to protect yourself from those. They're especially good for young people because they promote computer security in an easy and fun, and easy to understand way.

So for younger kids, Carnegie Mellon has developed an online safety site for games. It's called The Carnegie Cyber Academy at Carnegiecyberacademy.com. That's a great place where they can learn about phishing, cyber bullying, and different things. But it's in a traditional online gaming type of environment that they're used to.

DHS provides leadership for acampaign they call Stop, Think and Connect at stopthinkconnect.org. And this campaign has several useful videos and tools to promote online security awareness as well. Similar sites like stay safe online.org provide awareness and information.

And for me, the games part is cool. Some of them are fairly simple games where they present you some information, and you might have a multiple choice question after. Some of them are a little bit more fun and have some neat graphics. And some of them are tuned for different audiences. Some are more kid-oriented or some might be more appropriate for your typical business professional, just simplified for somebody that doesn't have an IT type of background.

Julia Allen: Okay. And what about someone who is looking for maybe a little bit next step after awareness? I know you've recommended a couple of publications and books that you think might be worth taking a look at.

Dennis Allen: Sure. So for those getting started in cybersecurity, I would encourage them to have a little fun doing it. Pick up a copy of *2600 Hacker Quarterly*. There's some fun books, like the*Stealing the Network Series: How to Own a Continent; How to Own an Identity*. Both of those are really useful because they expose you to different tools, techniques, and methodologies. And more importantly, scenarios in which those tools and that type of activity might take place.

Once you understand that scenario of how that could happen, it gives you a better perspective on what you can do to protect yourself and protect your infrastructure from those types of things.

Julia Allen: Some of these resources actually put in live situations or simulated situations where you have to pretend that something bad is happening to you, and you can actually work your way through a problem set?

Dennis Allen: Yes, absolutely. It gives you scenarios. So like the*2600 Hacker Quarterly* might give you an example; and again, some of this stuff is vetted. Obviously, in these two publications they are. You have to be careful with some of the things or resources that you have available. If you go right to YouTube and you start looking at videos that you think might be teaching you the appropriate things, they aren't necessarily doing that.

Some of these other articles do go through a vetting process to make sure that they make sense, that the techniques are actually verified, and that they work. And a resource site such as *Stealing the Network Series*, you're actually-- it's a whole book written by experts in their field and compiled in a story that makes it a fun scenario to go through, much like a movie is.

So that's another thing that you can do is you can take advantage of some of the films that are out there: films like Sneakers, The Net, even War Games with Matthew Broderick from the '80s, Firewall, Hackers. Some of these things are-- they're fun to watch. But you have to understand that not everything in there is real. It's a movie. So it might be enough to spark interest. There might be some real-world examples.

For example, in The Matrix they used a tool called Nmap or Network Mapper. That was shown on one of the screens in one of the scenes and everybody in the security world was like, "Oh wow, did you see they had Nmap running on there?"

And so there are some movies that do try to incorporate some pieces of realism to them. But mostly these are just really fun for you to go in and get a different experience, and try to figure out what makes sense and what doesn't make sense in the movie in terms of information security. And that's kind of fun.

Julia Allen: As we were preparing for this podcast, I know you had some great places for folks who are in more of a professional capacity; places where they might take a look. Can you mention a couple of those?

Dennis Allen: Sure, sure. There's professional organizations, like the Information System SecurityAssociation (ISSA). They release a monthly journal, which is great for CIOs (Chief Information Officers) and CISOs (Chief Information Security Officers) that gives you all kinds of information security events, information security news. It's more business or high-level oriented. Those are great places to go.

Certainly there's a number of Twitter feeds. Our society has become very social networking aware, and relying on social networking including Facebook and Twitter. But there's a number of great Twitter feeds out there from even some security vendors that give you real-time access to threat information. And those are a great place to go.

And of course there's what we have at CERT. We've got great technical reports, white papers, and this podcast series that are all available for information security professionals and business leaders.

Part 2: Gaining Practical, How-To Experience

Julia Allen: Great. So certainly plenty of information, depending on what your interests are.So let's say that I've done a little bit of homework. I've tried out some of these general resources that you've described and I really want to start building my skill base; that I've decided that it's worth investing in. So I know we're a great proponent of learning by doing.

So what do you recommend to folks who want to start to get their hands a little dirty and get some practical experience? What do you think is a good way to ease into this?

Dennis Allen: Well there's certainly the formal education route. A lot of places are starting to include operating system classes or network fundamental classes. There's no substitute really for on-the-job training. Depending on where you're working and what environment you're in, the opportunities for that may be a little greater than some others.

But really just messing around --creating your own sandbox, if you will, where you can have VMware or Virtual Box from Sun/Oracle. Learn how to actually install Linux operating systems and Windows operating systems. How do you download a CDimage, an ISO file, and run that within that virtual environment? Download firewall distributions.

There's a great one from Endian.There's a community edition, which is a free edition. Endian is e-n-d-i-a-n. There's a great edition that you can pull down and you can install that within your virtual environment, access that console. And just playing around in there, you're going to pick up as much as you would in a lot of formal courses. You can learn about access control lists, and proxy and filter capabilities, intrusion detectionand network monitoring, antivirus features. There's lots of things that you'll learn just be getting in there and playing around on one of those consoles.

Security tools distributions, like BackTrack; that's a great one. And it has become -- I won't necessarily call it a standard but I guess -- a de facto standard, if you will, in the security community. You need to be able to download that ISO file, make yourself a CD ROM, boot that CD ROM, either on a system or boot it in your virtual environment. Be able to play around with those tools. Learn how to use pretty much all of the tools that are on there, what they do, what bad guy might use them. It's a definitely a great place to start.

Julia Allen: And if I'm not quite facile with some of the recommendations that you've just made, are there some resources that can help me become better at applying some of these technology resources you described?

Dennis Allen: Absolutely. Especially for high school and college students, there’s plenty of opportunities. There's a website, uscyberchallenge.org and they actually have information about cyber camps and cyber quests.There's national high school competitions like Cyber Foundationsand Cyber Patriot. There's the National Collegiate Cyber Defense Competition.

Those are great placesto go to get information about those competitions and then work with your, again your high school or your college to try to get involved in one of those. And those are great opportunities to learn how to use these computer security tools and these technologies and really develop your skills.

Julia Allen: Great, great. Okay, so I'm armed, I'm ready to go. I've probably got enough information to be dangerous. My grandmother just called and said, "Can you help me? I have this virus or I have something bad that happened to my computer." So obviously helping your family is one way to go. But are there some other ways to actually begin to apply, take all these new skills for a test run?

Dennis Allen: I still get calls all the time from my neighbor and I can trade computer services for snow plow services in fabulous Rochester, New York – that type of thing. It works out quite well for me. But there's places like On Guard Online I mentioned already. They have a link in there to tutorials on information for securing your home networks -- very, very great.

If you are looking to secure your Linksys or your net to your wireless home router, change Windows passwords, those types of things, that onguardonline.gov site is very good with some tutorial videos to help you get started on that.

Securitytango.com is another one that has a lot of tips.If your computer is running slow, it tells you different things about deleting temporary files or disabling system restore, or links to antivirus or anti-malware types of applications to help you get cleaned up.

The one thing if you do get into doing the helping out your neighbor or your relative type of work, you need to be very careful.

First of all, don't plug a computer into your network that you know is bad. If somebody comes to you and says,"Hey, there's something wrong with my computer; can you check it out?" the first you should do is not plug that into your network. Make sure you have either an isolated connection or don't use the internet at all. Have your tools, utilities, on a CD that you can use to try to do some initial cleaning. Don't put that into your network.

And then remember, there's somethings that you can't un-see. There might be some personal informationon there – pictures. Or there might be something that you think might be illegal. Cybercrime.gov is a great site to go to get information about reporting different cyber crimes. And in some cases if you see something that you think is illegal, you may be required to actually report that.

And there's also again the potential of privacy or liability issues if you do break something or you make it worse. So be careful with that. And probably another really important piece is don't go rogue. Don't download these tools. Don't download BackTrack, like I mentioned, and start running these things on your college network or your home network or your work network. Because in some cases this might violate terms of service, acceptable use policies. Or you may even end up doing something illegal, even if on accident. So make sure you're playing in your own sandbox and you gain the expertise you need in that isolated environment first.

Julia Allen: Those are all great suggestions. It does-- as I'm listening to you talk though, it does feel a little bit overwhelming. There's a lot to learn; there's lots of opportunities to apply. And out of perhaps no ill intent, there's chances to get yourself in trouble without even realizing it. Right?

Dennis Allen: Absolutely.Yes, you definitely need to be careful and work, like I said, in an isolated environment. So understanding how to use those virtual technologies is a great place to get started.

Julia Allen: And do you find that there are -- like I'm thinking of mentoring. So do find that there are some on line forums where you can say, "I have this problem" or "I'm trying to experiment with this kind of approach" where you can actually get some advice from some more experienced hands?

Dennis Allen: There are some. You do have to be a little careful. Like I said, there are a number of Twitter people, or people that you can follow on Twitter, or people you can friend on Facebook, or blogs. You just need to make sure that you're getting things from reputable, trusted sources.

You don't want to end up running around in the wrong circles. Because the big difference between your typical black hat bad guy versus your white hat good guy is not necessarily in the knowledge that you know. It's how you apply those tools and what you do with your knowledge.

Julia Allen: Right. And it occurs to me that you'd want to also make sure that you don't inadvertently get involved with a bad crowd, so to speak. So you start asking questions, and they start to see what kind of skills you have, and all of a sudden you find yourself in a situation where you're being recruited to do things that you never intended, right?

Dennis Allen: Absolutely, absolutely. Yes, and that's a big point. And actually we can talk about that one too. And you see folks like with Albert Gonzalez that was a cybercriminal, if you will. He had got in trouble.

But with a big incident that happened, the TJX incident that involved Heartland Payment Systems, JC Penney, T.J. Maxx and others. He didn't work alone. He had other associates that actually wrote computer exploits that were experts in wireless hacking or that could create the fake credit cards.

So there-- it's not one individual working alone. It's people that have various levels of expertise that are getting assembled to actually do these sorts of things. So you could easily find yourself in the wrong forum or with the wrong crowd, trying to learn something that you're trying to use for purposes of good, not evil. So you got to be careful.

Part 3: Pursuing Formal Education and Certification

Julia Allen: Excellent advice. So let's-- as we come to our close, Dennis, can you say a little bit about how you take this emerging interest and skill set and actually seek out opportunities for formal education or certification, where you can start to actually develop some credentials that are recognized so you can work yourself into a professional position doing this kind of work?

Dennis Allen: Absolutely. Well a college education is going to be very important for career advancement. A bachelor's degree, a master's degree in information assurance or computer science is definitely going to help you out -- not just for career advancement, but it's gives you a solid foundation of skills and techniques that you can use throughout your career: the troubleshooting skills; the ability to evaluate logic problems or programming flaws.

And programming classes in Java, C, or Python or others are really good for helping you develop those skills. Those break fix --break fix, fix cycles of learning -- they really can help contribute to the success of an IT professional.

But if you don't pursue that degree program, taking a programming course at a community college or an operating system course at a community college is also another good way to get you started. Full curriculums now for the cyber warrior, if you will, still rely a lot on that traditional "Hey you need to have mathematics and programming and operating systems and network architecture, and all these other things."

But very few really get into exploring the way the bad guy thinks or the development of malicious code, if you will. There are some professional programs out there now, certification programs or career paths, that allow you to get into that outside of that outside of the university system.

Julia Allen: Right. Because-- just as an aside-- in our software assurance work and in building education to help developers develop more secure, robust software-- I think you hit the nail right on the head.

We're thinking like an attacker, thinking like a bad guy, and trying to anticipate what they might do -- that's not taught anywhere or that's really not a common way of thinking when you're trying to build or assemble or integrate or deploy a system, right?

Dennis Allen: It's not. Because we're still looking at it from a professional development piece, right? We're talking about formal education because that's going to help us get paid.

We're talking about security certifications, (1) because there's a DoD directive -- the DoD Directive 8570 for training, certification, and workforce management -- that tells us that if we're a certain level technician or manager, we might have to have our CISSP credential or our Security+credential, or in some cases our Certified Ethical Hacker credential.

And all of those are necessary for the position we're in, or advancement, or to get paid. So a lot of times our objectives are different than the bad guy or cyber attacker community. Because they're able to focus their efforts on one particular thing.

I mentioned Albert Gonzalez. In that scenario he's working with other people that are experts at doing a certain thing, like writing an exploit or wireless hacking. It's very difficult for today's cyber warrior, whose goal is to have this breadth of knowledge. But it may only be an inch or, if they're lucky, a foot deep.Whereas our cyber criminals are actually having, maybe not the breadth of knowledge, but they have an enormous depth of knowledge.

We need to be able to develop cyber professionals that actually have that breadth of knowledge but also have that depth of knowledge in one or two areas where they can actually be innovative. They can be ahead of the game or at least on par with some of these criminals.

Julia Allen: So what you're saying is obviously you have to have the knowledge base from which to draw. But you're also highly recommending, like most complex professions, that cyber warriors pick a specialty. Pick something that they are—like forensics or like intrusion detection or maybe like network situational awareness -- that they pick something that they have a lot of depth in and a lot of hands-on experience with.

Am I hearing you correctly?

Dennis Allen: Absolutely, absolutely. And one of the key things not to lose out is that us as business leaders, or cyber generals if you will, need to understand where these areas of expertise are. So if we need to call upon somebody that needs to do awireless attack or a incident response to a wireless attack, we need to know where that expertise is. And it may be in a sister organization or it may be some place outside of my direct management.

But I need to understand who else has that expertise that I can call upon in those types of emergencies. And it's the same thing for government agencies. There needs to be better collaboration between our law enforcement agencies to work with one another and develop those expertise to support one another. And I think that is happening.

Julia Allen: Well Dennis, I feel like we've barely scratched the surface.And I can't thank you enough for all the preparation and all the great resources that you've pointed out, across the spectrum of-- from just the very beginnings of thinking about, learning about this field, all the waythrough to applying the skill sets.

So I'll give you one more chance though. Do you have any additional resources that you'd like to call out? And we'll put links for all of these in the show notes.

Dennis Allen: Sure. One of the things that I would do is I would google 'DHS' and then ‘cybersecurity’. That gives you a link that we'll have in the show notes already for you. But that has some resources for you to get started.

The U.S. Cyber Challenge site that I mentioned, uscyberchallenge.org, is a great place for high school and college students. Make sure you take a look at that, us-cert.gov is a great place to go. Our CERT site that we mentioned. Lots of training that we have available: public training classes, workshops that we do, the podcast series, and much more.

And then a particular site that's with the folks in my particular workforce development area. We have a site, xnet.cert.org. And that, among other things, has some white papers on there that go through our approach to the cybersecurity workforce development --the whole building of knowledge, skills, experience and evaluation. We got those white papers there, as well as a demo to our training environment that helps you build that experience to make you an effective cyber warrior.

Julia Allen: Excellent resources, Dennis. Again, thank you so much for the introduction to this very challenging, very exciting, and very complex field. I thank you so much for your time today.

Dennis Allen: Thank you.