CyberPro

Volume 7, Edition 5
March 6, 2014

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Lewis Lightner, Director, National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition

NSCI recently had the opportunity to interview Lewis Lightner, Director, National Cyber Watch Mid-Atlantic Collegiate Cyber Defense Competition (CCDC). The Mid-Atlantic CCDC is a competition composed of college/university student teams from the Mid-Atlantic region. The competition focuses on the operational aspects of managing and protecting an existing network infrastructure. Throughout the competition, each team has to ensure their systems supply specified services while under attack from a Red Team (Hackers). This event is a regional qualifier for the National CCDC.

NSCI: Can you tell us a little bit about the National CyberWatch Center and Mid-Atlantic Collegiate Cyber Defense Competition (CCDC)?

Lightner: The National CyberWatch Center is a National Science Foundation (NSF) funded Advanced Technological Education (ATE) center. Our mission is to lead collaborative efforts to advance cybersecurity education and strengthen the national cybersecurity workforce. Originally funded as a regional ATE center in 2005, a new National Center ATE award was funded by NSF in the fall of 2012.

The Mid-Atlantic Collegiate Cyber Defense Competition began as a project within the CyberWatch regional ATE center in 2006. The Mid-Atlantic CCDC is unique in that it focuses on the operational aspects of managing and protecting an existing network infrastructure. The teams are physically co-located in the same building. Each team is given physically identical computer configurations at the start of the competition. Throughout the competition, the teams have to ensure the systems supply the specified services while under attack from a Red Team. In addition, the teams have to satisfy periodic "injects" that simulate business activities IT staff must deal with in the real world. The competition objectives are to:

- Build a meaningful mechanism by which institutions of higher education may evaluate their programs;
- Provide an educational venue in which students are able to apply the theory and skills they have learned in their course work;
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams;
- Open a dialog and awareness among participating institutions and students.

NSCI: What kind of impact have you seen on interest in cybersecurity or cyber-related education in general as a result of the Mid-Atlantic CCDC?

Lightner: Students participating in our competition experience the real-world. They're expected to not only defend their systems, but also perform the routine duties that anyone working in the field would be doing. This gives them a taste of what the workforce will be like. As a result, we see a lot of students who weren't necessarily looking for a career in cybersecurity before the competition come away with a new found interest. They discover that the field requires a great deal of strategic thinking and the ability to get outside of the box with unique solutions. A lot of cyber, and IT related education in general, has been tech heavy; neglecting the need to develop the thinking and decision making process within the student. Rather than presenting a student with a task requiring them to complete a series of predefined steps, we should be simply telling them to solve a problem. Part of the learning involved with the latter is that the students develop the steps required to solve the problem instead of being presented with them beforehand. Instructors and others who attend our competition see the importance of this method of learning and are starting to envelope it into teaching strategies.

NSCI: Can you tell us about any incentives the National CyberWatch Center provides to encourage cybersecurity education?

Lightner: Cybersecurity education is what we're all about. We advocate for the role of community colleges in cybersecurity education and workforce development; we build novel solutions for our nation's cybersecurity education and workforce development challenges; we collaborate with educational institutions, businesses, government entities, and professional organizations to strengthen cybersecurity programs nationally; we coordinate and support regional and national cybersecurity education programs and; we promote educational and workforce development models of excellence. Our goals are focused on cybersecurity education at all levels--from elementary through graduate school, but especially the community college level, and include the following:

- Building a culture of collaboration;
- Building, collaborating, coordinating, and promoting program, faculty, and student capacity based on models of excellence;
- Promoting the cybersecurity field;
- Advancing research in Practice-Centered Cybersecurity Education.

NSCI: What are a few of the current significant challenges or gaps you see in cybersecurity education?

Lightner: Awareness of the need for cybersecurity education is a big problem. Not only does the issue exist in attracting students into the programs, but there are also difficulties establishing the programs themselves; which is not an easy problem to solve. Everything from funding issues to finding qualified faculty contributes to the issue. Projects within the National CyberWatch Center are making efforts to try to address some of the challenges.

- We are working collaboratively to create and/or identify national models that will make it easier for students to progress from a 2-year degree to a 4-year degree;
- We are conducting research to try to understand exactly how students need to prepare for entry into the workforce.

- We have developed many resources to promote cybersecurity education at the K-12 level to generate interest in the field at a younger age;
- We are helping colleges better understand the different training standards that exist and incorporate these into their programs of study.

NSCI: Can you talk about the challenges with attracting students to tech-heavy fields like network security and software development?

Lightner: I've had many conversations with people who press the mute button once they find out I'm talking about something to do with computers. A lot of your readers have probably experienced the same thing. Unfortunately, the uninformed don't fully understand what it takes to work in these fields. Every job does not require a computer science degree that involves successfully completing four semesters of calculus. This is part of the challenge that the National CyberWatch Center is trying to address. It is extremely important that every organization employ people that are qualified to perform the tasks they are assigned. However, in a lot of cases those same people are over qualified. Work has been done to identify the knowledge, skills, and abilities (KSAs) required for the job roles within the cybersecurity workforce. Now we need to establish exactly what the training and education requirements are to acquire the KSAs. The resulting information must be widely communicated so people understand that they don't necessarily need to be a rocket scientist to do this kind of work.

NSCI: What areas would you say are the most valuable or interesting to cybersecurity students?

Lightner: The most valuable areas are the things they learn in their basic cybersecurity courses. Establishing the foundation is key to understanding more advance topics. We see competition teams do poorly all the time because they didn't pay attention to basic information security principles such as changing default passwords, closing unused ports, and applying patches. The most interesting area for students, without a doubt, is penetration testing. Students like the challenge of trying to do something that is somewhat clandestine.

NSCI: What area of cybersecurity do you see as having the most potential for growth or opportunity for students in the near future?

Lightner: In the next ten years I expect the lack of qualified personnel to be addressed by most players within the cybersecurity industry. As the threat of cyber-attacks increase, the need for qualified personnel and modernization of equipment and technology also goes up. While the United States leads the global cybersecurity market in all areas, the percentage of spending weighs heavily toward network security in most areas of the world. This trend is expected to continue. Students preparing for a career in cybersecurity should pay close attention to the defense segment.

NSCI: What changes would you like to see to better prepare cybersecurity students for eventual transition to jobs (e.g. government, financial, national security sectors)?

Lightner: We need more collaboration among all players. The nature of how we connect externally bounds us to common adversaries. Public and private sector have got to work together to create models that will guide how students need to prepare. It doesn't matter if we're tasked with protecting credit card data or matters of national security. The knowledge and skill needed to secure it are the same. Developing common standards of training and education will ensure students are prepared for jobs no matter where they become employed.

NSCI: Is there a particular balance between cybersecurity education, certification, red-teaming exercises, etc. a cyber-professional should pursue to best develop and maintain their education and technical skills?

Lightner: I like to visualize it as an equilateral triangle. Education, certification, and experience are all equally important. Colleges and universities can provide the first two but we have to rely on our industry and government partners to provide opportunities for students to gain experience. If we expect to make a dent in the need for qualified personnel, more colleges and universities will need to offer quality programs in cybersecurity and more industry and government partners will need to play a larger role in providing students with practical experience.

NSCI: Is there anything else you'd like to add?

Lightner: Thank you for the opportunity to share my views on these important issues. If anyone is interested in learning more about the Mid-Atlantic CCDC or the National CyberWatch Center, they can contact me at maccdc@cyberwatchcenter.org.

NSCI: Thank you very much for taking the time to visit with us.