CAMPUS TECHNOLOGY

Security Initiatives

Cyber Challenge: 10,000 Security Warriors Wanted

- 05/14/10

Karen Evans understands the need for online security--and for people who really know how to implement it properly. Evans, who spent 28 years with the federal government in the Office of Management and Budget as administrator for e-government and IT and CIO for the Department of Energy, among other positions, was in charge of a project during the Clinton administration to bring Internet access to the Department of Justice. Then-Attorney General Janet Reno wanted to be able to send and receive e-mail in the department and to set up an agency Web site. In August 1996, on the weekend before it was supposed to be moved to a 24x7 data center, the site was hacked, and Reno's picture was replaced with a picture of Hitler. This most infamous of hacking incidents (probably caused by a CGI vulnerability) was a "really good wake-up call for a lot of people," Evans said, "including my management. It was instrumental in helping me think through how to manage an IT and online services of portfolio."

As Alan Paller, research director for the SANS Institute, has written, that particular defacement had a major impact because it forced Evans "to become an expert in the technical aspects of cybersecurity, and she has subsequently had more positive impact on federal cybersecurity than almost any other federal [employee]."

That's why, when the policy institute called the Center for Strategic & International Studies put together a commission on cybersecurity for the Obama administration, Evans was asked to join. Likewise, when that commission decided to address the human capital issues--an insufficient number of people with the right skills to perform security work--Evans was again invited to participate, this time as the head of a new program called the United States Cyber Challenge.

As a report produced by the commission explained, "The cyber threat to the United States affects all aspects of society, business, and government, but there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the [f]ederal [g]overnment. [Using an] airplane analogy, we have a shortage of 'pilots' (and 'ground crews' to support them) for cyberspace." As Evans put it, "You can have all the tools you want. But if you don't have the right people with the right skills, it doesn't matter."

The Cyber Challenge, which is part national talent search and part skills development program, has set a goal of finding 10,000 Americans with the skills to fill the ranks of "cybersecurity practitioners, researchers, and warriors." The idea, Evans said, is to nurture and develop participant skills, give them access to training and practice, and give them exposure to colleges and employers "where their skills can be of the greatest value to the country."

The challenge is being put to the test this summer in an alpha run. Participants in California, New York, and Delaware can try out a free online treasure hunt, developed by SANS, an organization that provides security training and certification. Those who pass muster will be invited to attend a summer camp in that state where they'll receive a week of training by SANS and university faculty and students.

The treasure hunt, which is open book and not timed, presents a fairly ordinary looking company Web site. But it has some security holes. Competitors are supposed to uncover those security vulnerabilities and then answer a set of questions.

But Evans emphasized that evaluators aren't necessarily looking only for people skilled enough to pass the treasure hunt challenge in the first try. "The treasure hunt allows you to play multiple times. Say the first time you come in, you do score 100. OK, we know they know this stuff. That tells us one set of things about a person and their ability to look at information," Evans explained. "But say another person comes in and only makes a 60. Then they keep trying. Say it took them 10 times, but they wanted to achieve 100. What you get from that is that they're pretty competitive with themselves and they want to make sure they're eligible. Those are the different things you look at when you're trying to figure out what makes for a good cyber professional."

Evans said she sees the whole project as having three components: community building for participants; "rack and stack" for identifying skills and interests; and matching up individuals with government agencies offering scholarships and industry offering internships and jobs.

She added, "You can't do this without the universities, since they offer additional education opportunities." That's where Cal Poly, the California State Polytechnic University in Pomona, comes in. When Dan Manson heard about the Cyber Challenge on a phone conference with members of California's state IT organization, he thought it was a natural fit for Cal Poly to host.

Manson is a professor of computer and information systems, as well as the director for the Center for Information Assurance in the College of Business Administration. "We've been hosting the Western Regional Collegiate Cyber Defense Competition since 2008. We really believe in learning by doing," Manson said. "So we think this is a great way to have students learn about cyber security--through competitions and challenges. We wanted to be a part of this in whatever way we could help."

Cal Poly will host its week-long training camp July 19 to 23. The other campuses that will host camps are the Polytechnic Institute of New York University (July 26 to 30) and Wilmington University in Dover, DE (August 9 to 13). All expenses--travel, housing, and meals--will be paid.

Attendees will get a major dose of training in intrusion detection, penetration testing, forensics, and other security-related topics. At the end of the week, the group will be broken into small teams to play a capture-the-flag competition for prizes and recognition. During that final day, Manson explained, all the contestants will be in the same big room, and each team will have a flag on its server. While they're trying to capture the flags of other teams by finding weaknesses in their systems, they'll also be defending their own. Plus, a wildcard "red team" separate from the student teams will be striking out with their own forms of attack.

As part of the pilot program, each camp will host 18 to 25 participants who live in or attend college in the state where the camp is being held. Eventually, the camps will also be opened up to younger people, but for this first effort, there's an age criteria. "Because of legal issues associated with high school age children and overnight stays and having chaperones, the group decided this year participants needed to be 18 years or older," Evans said.

That points out another aspect of this program that makes it different from other types of security competitions. Participants don't need to be students at all. "We're trying to grow the pool," Evans said. This includes attracting adults "looking to be re-employed."

Kyle Osborn, a 19-year-old who holds two jobs in IT and takes classes in Orange County, California at Golden West College and Cypress College, has tried out the treasure hunt. His impressions (without giving away the answers): "There were a few things I wouldn't have been able to find out unless I was really looking for them. I did learn one or two things from it. That was nice."

Osborne became interested in cybersecurity as a 16-year-old, and he has participated in other cyber competitions, such as the Cal Poly Collegiate Cyber Defense contest. So he knows he has an affinity and interest in what the Cyber Challenge is trying to accomplish. But, he pointed out, "There are people who are interested but don't know how to pursue it and get into it. This will help a lot of people that way. Having 25 students that are all interested in the same material, in the same career profession, inside the same room for a whole week, I think it'll be a lot of fun."

Evans and the others have ambitious plans for the program. After all, the goal is 10,000 security warriors. That means expanding to every state. "In this alpha run, we'll work the bugs out," she explained. "It would be really bad if we tried to do one in every state and fell flat on our face. The idea is that once we get this first set going through, then we'll have a toolkit and framework so that we know how to scale it out. It would be really great if every college were running a camp in the summer."

Initial funding for the program is coming from CSIS and SANS. But one of Evans's jobs is to build out the organization, make the program self-funding through industry and government sponsorships, and also to move it under an existing entity such as the non-profit Center for Internet Security, on whose board she serves.

"What happens here is that everybody benefits," Evans said. "All of these organizations--industry and government--ultimately benefit at the end. What I'd like to get to five to 10 years from now is that we have enough people who can do all of those jobs. Everyone shouldn't have to live through a hacking incident like I did. That's a great learning experience, but we don't want that to happen to everybody."

About the Author

Dian Schaffhauser is a writer who covers technology and business. Send your higher education technology news to her at dian@dischaffhauser.com.