the cyberwire

The CyberWire
621 East Pratt Street, suite 300
Baltimore MD 21202–3140
editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire

The National Initiative for Cybersecurity Education Conference

November 5-6, 2014 Columbia, MD

November 5

The National Initiative for Cybersecurity Education (NICE) conference opened in Columbia, Maryland this morning. Rick Geritz, LifeJourney CEO, welcomed the speakers and other symposiasts. He sees the cyber industry, and cyber education, as having arrived at a tipping point. Cyber attacks are driving broad realization of the need for cyber security, and the concomitant need for a trained and educated labor force that can meet that need.

Russell Shilling, Executive Director of the US Department of Education's STEM (science, technology, engineering, and mathematics) education effort, delivered the morning keynote "Ready to Work." As his title implied, the Department of Education's STEM programs are indeed aligned with the broader federal "Ready to Work" initiative. Shilling stressed the importance of starting STEM education in general, and cyber education in particular, as early as possible — elementary and even pre-Kindergarten programs are vital to students' future readiness for careers.

Shilling also offered some thoughts on educational program designs. Good programs should scale readily so that they can be delivered to the largest possible number of students. Cyber security skills, and therefore education, have a brief shelf life. Effective STEM curricula, then, should inspire students to continue learning throughout their lives.

Shilling suggested that effective story telling is an easily overlooked and neglected aspect of education. He's seen both games and graphic novels used to good effect, but the stories must be well told and engaging, not merely a thin framework on which traditional curricular content is stretched. He also advocated for the early and continuing infusion of social and ethical awareness into STEM education, and argued that such awareness is particularly important to cyber.

The Department of Education has STEM priorities in over sixty programs, Shilling said, and these afford great scope for academic cooperation with both industry and government. He advocated use-oriented research conducted by diverse teams, saying that in his view every organization needed its own version of DARPA. The Department of Education is interested in working through the SBIR (Small Business Innovation Research) program, and also hopes to foster internships.

Shilling concluded by commending some models that the cyber sector might follow to its profit. The Maker Movement offers a good model for packaging education to both teachers and students, and for easy company engagement. Another very positive model in STEM to STEAM is CS2N, particularly its robotics components, and also its contributions to teacher training and certification.

Benjamin Scribner (Program Director, National Cybersecurity Professionalization and Workforce Development Program at the US Department of Homeland Security) followed with an address to the general session about the National Cybersecurity Workforce Framework. He made the now customary gesture toward making our flesh creep with tales of growing threats and our rapidly expanding attack surfaces. Cyber predators milk seniors out of savings, lure children into crime, and use the Internet to steal and embezzle, killing businesses and jobs as they do. Cyber attacks threaten a way of life that depends upon the reliability and availability of critical infrastructure.

His sound point in covering this ground was to point out that a new awareness of the threat is driving the young cyber labor market. That new market's professions remain ill defined with unclear career paths, and this lack of definition and clarity itself contributes to labor shortfalls. The National Cybersecurity Workforce Framework addresses the immature professional labor market by providing a common cyber taxonomy and lexicon. A well-structured profession will enable and encourage participation in the labor market. He closed by commending NICCS communication tools to academia and industry.

Several of today's afternoon sessions took up issues of certification, and, more generally, the challenge of determining that cyber workers actually have the skills necessary for their jobs.

Organizers of cyber competitions described how competitions support and inspire STEM education. Such competitions are vehicles to support the larger STEM workforce's growth over time, but they also seek to redress immediate labor shortfalls. If competitions help schools teach essential skills, students will find that careers follow. In any case, precise career planning is difficult: stories, panelists agreed, were much more useful.

A panel on certification took pains to distinguish certificates from certifications. Certificates confirm learning. They're not tested, validated, or aligned with needs, as are certifications.

Certification is inevitably bound up with professionalization. Resolving current confusion over which certifications are valuable depends upon first recognizing that one can't professionalize an entire field as disparate as cyber security. There are too many types of jobs. We professionalize occupations to remediate deficiencies, and so we should begin in cyber by identifying occupational deficiencies, and only then evolving standards and practices to remediate them.

The medical profession offers a good analogy for cyber: there are many disparate occupations (consider nurses, surgeons, etc., and the various specialties within those careers.

All professions place entry-level practitioners in a safe environment under senior supervision. So should cyber. And all cyber specialties aren't equally mature, or equally crucial. Recognizing this should shape professionalization. Certifications, to be adequate, must capture craft elements of occupations, and verify that cyber practitioners have them.

A session on Centers of Academic Excellence continued this line of thought. Such centers are attractive sources of cyber labor because their graduates are known commodities.

November 6

The conference's second and final day was opened by LifeJourney CEO Rick Geritz, who reported on yesterday's meeting of the NICE 365 Board (a corporate advisory group). There was considerable interest in and commitment to STEM education; the challenge now is coordinating corporate support. Geritz introduced one coordination aid: the online NICE Cyber Education Map, an interactive tool showing cyber education programs.

Howard Community College President Hetherington spoke next, describing a cyber education role for community colleges (her own college, of course, furnishing examples thereof). She emphasized the importance of "soft skills" education to cyber, and the importance of integrating it into STEM programs. (She noted that ethics and communication were particularly important.)

USA Today's Vinnie Polito delivered the morning keynote, "Why Cyber Security is STEM." He noted that unemployment is, in many ways, a supply-side problem: many remain unemployed because they lack skills, and that lack of skills creates the cyber labor shortage. Skill training, including key craft skill training, should begin in middle school and high school.

There's no lack of expressed commitment to STEM education. "USA TODAY has been covering the education market for decades," Polito said. "There's a STEM program for every conceivable interest group." But too many of these are one-offs, and haven't shown an ability to scale. We're in a post-Sputnik moment with respect to national concerns about STEM education. But worry won't serve as an effective spur to action unless we develop the ability to develop and scale educational best practices.

In sessions held during the conference's final day, symposiasts continued to advocate rethinking cyber training and qualification along the lines of traditional craft apprenticeships or supervised practice analogous to medical residencies. Others expanded on early descriptions of the importance of storytelling — effectively, ideation — in attracting students to STEM careers.

Jay Bavasi, President and founder of the EC-Council Foundation, closed the conference with a keynote entitled "Ready to Work: from Zero to Hero." Ready-to-work initiatives seek to address and solve an industrial labor force shortfall. But in cyber security, Bavasi argued, we're generally still fixated on responding to incidents. If we dissect the problem, it's evident that, without vulnerabilities, there's no hack.

Customers (according to software industry executives Bavasi talks to) want affordability, functionality, and ease-of-use, but they don't initially focus on security. The day hacking becomes a problem, and then the mentality is that they'll deal with it. This mentality isn't conducive to development and delivery of secure software — the market doesn't push for secure design.

This, in Bavasi's view, is a failure, because security can and should be addressed in development. An EC-Council Foundation study found that some 96% of colleges worldwide had no secure programming requirement. In many, it's not even an elective. The foundation decided to investigate a test case to gain some insight into whether colleges and universities were in fact producing secure programmers who were ready to work.

Taking India as a test case (and Bavasi was at pains to stress that India was a sample, and offered to wager "all the money I have" that results anywhere in the world wouldn't differ significantly), the foundation organized CodeUncode to look for the top secure programmers in that country. Taking a sample of roughly 10,000 players, the exercise found fewer than 1% skilled in secure programming.

Such dismal results were a national scandal. (Again, India is by no means unique — much the same would be found everywhere else.) Looked at differently, the outcome was even more dismaying. About 13% of the graduates who participated were trainable, but 86% were effectively unemployable. Basic knowledge was far too rare: understanding of error and file handling were particularly deficient.

The Indian government responded by requiring colleges to address cyber security in their curricula (but failed to specify what, exactly, that meant).

If, Bavasi argued, we're serious about getting students ready to work, we should first stop manufacturing the problem: insecure code. We need to gamify, for example, secure software creation, and train students to avoid coding easily exploited vulnerabilities into their programs.

He turned to considerations for companies hiring cyber experts. He advised they look for loyalty, a good track record, mission readiness, and technical ability. Wounded warriors have all these except the last — technical ability. That, of course, we can give to them if we commit to supporting their training and education.

Bavasi concluded with two calls to actions. He asked faculty and industry to insist on secure coding. And he called on everyone to support technical scholarships for wounded warriors.

the cyberwire

editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire
+TheCyberWire

About The CyberWire

The CyberWire is supported by CyberPoint International and its community partners. We invite the support of other organizations with a shared commitment to keeping this informative service free and available to organizations and individuals across the globe.