CISSE K-12 Cybersecurity Education Summit Overview

The summit goals are described in this paper and are intended to be shared with participant invitations. It is meant to be fluid and will be updated based on feedback and suggestions.

Background

Information technology has moved beyond a luxury solely for businesses; it has become an integral part of the modern world. It is ubiquitous outside the formal classroom setting and is becoming a universal part of the K-12 environment. Technology clearly has brought a large number of positive effects to the educational community, including improved access to information; improved simulation capabilities, enhanced productivity, and a means to provide technology based assistive support. In spite of these advances, technology has also brought challenges.

The Director of National Intelligence (DNI) testified before Congress, stating: "The growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures. The Intelligence Community assesses that a number of nations already have the technical capability to conduct such attacks."[1] The globally-interconnected digital information and communications infrastructure known as "cyberspace" underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security. Cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century. These challenges are captured in U.S. Bureau of Labor Statistics (BLS) employment projections. Overall, the BLS estimates total U.S. employment to increase by 10 percent from 2008 to 2018. However, cyber related jobs are expected to grow at significantly higher rates. The demand for cybersecurity professionals is estimated to grow to 2.5 million new workers by 2015. The need for network systems and data communications analysts is expected to grow by 53.4%, and the need for computer software engineers is expected to grow by 34% over the same time period. The BLS attributes this growth to the increased need for workers with information security skills. Overall, the BLS estimates computer and mathematical science occupations will grow by 22.2%. This parallels similar data for almost all STEM fields[2]. Clearly, the available workforce is not growing with the demand. The gap between supply and demand in STEM and particularly in the growing cybersecurity field is a national problem.

At the same time, there has been an exponential growth in cybercrimes reported to the FBI since 2000. In 2000, 16,383 were reported; and 275,284, 336,655, and 303,809 crimes were reported in 2008, 2009, and 2010 respectively. The most frequent crime was credit/debit card fraud, however intrusion, spam, and child pornography were also frequently reported. Commercially, losses attributed to computer security issues averaged more than $230K per organization in 2008[3] with over 60% of the losses being attributed to non-

---

[1] Cyberspace Policy Review (2009). Assuring a Trusted and Resilient Information and Communications Infrastructure http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

2 Additionally, a study in 2008 by the National Science Foundation found that the number of graduates with science and engineering degrees, at the bachelor's level or higher, increased by an average rate of 1.5 percent a year from 1980 to 2005. But the average employment growth for such jobs each year over the same period was 4.2 percent.

[3] Richardson, R. (2008). 2008 CSI computer crime & security survey: Results from the longest-running project of its kind, Computer Security Institute.

malicious actions by insiders. The FBI, CERT, and (ISC)2 prioritize education and awareness before technical interventions in protecting users and infrastructure.

Increasing public awareness about cybersecurity and increasing the U.S. technologically advanced workforce are two priorities spelled out in the President's 60 Day Cyberspace Policy Review (2009)[4]. As referenced in the report, the U.S. should initiate a K-12 cybersecurity education program for digital safety, ethics, and security; expand university curricula; and set the conditions to create a competent workforce for the digital age[5]. To achieve these goals, the report suggests: 1) initiation of a national public awareness and education campaign to promote cybersecurity risk awareness for all citizens; 2) changes in the educational system that will help enhance the understanding of cybersecurity and allow the U.S. to retain and expand upon its scientific, engineering, and market leadership in information technology; and 3) development of educational opportunities and strategies that will expand and train the workforce to protect the Nation's competitive advantage, including attracting and retaining cybersecurity expertise in the Federal government. The report goes on to state, "The Federal government, with the participation of all departments and agencies, should expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy. Existing programs should be evaluated and possibly expanded, and other activities could serve as models for additional programs."

People recognize the need for curriculum and professional development throughout the K-12 through post-secondary pipeline, but there are limited efforts to coordinate and document on-going efforts. There are many endeavors at the local, state, and national level, but there is a lack of clarity with regards to what topics are being addressed, what groups are delivering the programs, and where they are in development. In some cases, many people are designing a program to address or target the same issue, target audience or demographics, whereas in other cases, topics, targets and issues are left unaddressed. While having multiple approaches is not in itself an issue, a gap analysis is needed to see what is not being addressed, and what areas may have duplicative rather than complementary programs. Additionally, there is a growing recognition that there is a difference between cyberawareness training and cybersecurity workforce education. For the purpose of this project, cyberawareness may be included within training, but the focus is on programs, efforts, and strategies to build a pipeline of workers with a foundation of information technology (IT) knowledge and skills to support cybersecurity.

Goals and Objectives

This event focuses on one part of the workforce pipeline continuum, the K-12 endeavors, and includes both informal and formal efforts.

It is part of a larger national effort to document the K-12 cybersecurity education programs on-going throughout the country and to address the goal: *to develop a comprehensive agenda focused on the challenges of cybersecurity education at the K-12 level.* Currently, many efforts are underway to encourage

4 Cyberspace Policy Review (2009). Assuring a Trusted and Resilient Information and Communications Infrastructure. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

5 Pruitt-Mentle, D. (2008) National Cyberethics, Cybersafety, Cybersecurity Baseline Study. http://staysafeonline.mediaroom.com/index.php?s=67&item=44.

students to explore cybersecurity careers. From these, what are the best ways to educate students, educators and parents about careers in cybersecurity and other Science, Technology, Engineering and Mathematics (STEM) related pathways, and what roadmaps can be drafted indicating both the resources required and the potential barriers that have to be overcome. We are particularly interested in:

- What is the nature and extent of cybersecurity education in U.S. K-12 schools?
  in extended learning experiences?
- Who are the major providers of cybersecurity education content in U.S. K-12 schools?
  in extended learning experiences?
- What is the perceived importance of cybersecurity education content for U.S. K-12
  school programs?
- What content is being delivered to students? educators? and how is it being taught?
- What, if any, are the issues and barriers that impede the delivery of cybersecurity
  education content in U.S. K-12 school programs? and
- How are current programs being evaluated (teaching and learning)?

Maryland, as a case study, served as the first in a series of similar events scheduled throughout the U.S. The second summit scheduled at the 16th Annual Colloquium, gives additional input from CISSE participants; including those connected with CAE and CAE 2Y institutions. In addition, focus groups will be formed to facilitate the collection of qualitative and quantitative data describing efforts and impacts of programs underway across the country.

This summit will explore the nature of cybersecurity education K-12 programs across multiple stakeholders, determine how to connect efforts into the larger whole, help establish improved program design, and provide the foundation for future studies either expanding particular subject areas or examining progress.

The objectives for the CISSE K12 Cybersecurity Education Summit are to:

- share successful activities;
- create a comprehensive list of on-going K-12 efforts from input from CISSE participants/CAE/CAE2Y and CAE-R institutions;
- examine efforts to identify what's working/not working and provide feedback on lessons learned; and
- identify gaps in our K-12 cybersecurity programs.

As with most efforts within the K-12 landscape, location, demographics, timing, leadership, and resources often dictate the success and sustainability of even the most robust and well-constructed programs. Activities can vary widely from district to district and between schools, not just from a content perspective, but as a result of the knowledge of the people running the program. We expect this effort to detail many possible approaches for delivering cybersecurity workforce awareness and development, and as a result, provide a catalogue of efforts, feeding into a gap analysis with regards to location, demographics, and content.

Formal vs. Informal

For the purpose of this project, formal education will be defined as a structured system of learning provided or overseen by a local or national entity for its citizens. A body of formal education is an accredited institution whose curriculum is answerable to an overseeing body of academic standards. In other words, what is taught in school as part of the formal content delivery. Informal education will refer to learning acquired independently through non-academic means. It can either mean that students are self-taught through their own reading and research, or through experiences, activities and programs, delivered outside the normal school day.

Cybersecurity Education

Cybersecurity has grown from a buzz word to the focus of many technology, education, and public policy initiatives. However, one conundrum is the lack of clarity regarding the definition of cybersecurity, especially as it changes based on context. For some, cybersecurity is explained to be the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cybersecurity. For this definition, elements of cybersecurity most often include: application security, information security, network security, disaster recovery and business continuity planning, and end-user education. The Merriam-Webster dictionary defines cybersecurity as*, measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack*.

But what does cybersecurity education mean, particularly within the K-12 environment? What does it include? Is it different when broached in the context of cyberawareness vs. workforce development? Should "it" be taught? If so, how should it be taught? as a "separate" subject area or mini modules embedded within other subject areas? Is it more appropriate to integrate within existing technology related content? Or should schools embed the higher level concepts into other curricula similar to engineering topics? When we encourage students to pursue a career in this field, what career path do we encourage them to take? Engineering? Computer science? Networking? According to the *Cybersecurity Workforce Framework*[6], "there is little consistency in how cybersecurity work is defined and described throughout the nation. The lack of a common language to discuss and understand the work requirements of cybersecurity professionals hinders our nation's ability to baseline capabilities, identify skill gaps, develop cybersecurity talent in the current workforce, and prepare the pipeline of future talent." Cybersecurity is a recent and rapidly developing specialty in government, and does not fit into the standard occupations, job titles, position descriptions, and federal job classification and grading systems managed by the Office of Personnel Management. This has made identifying, educating, recruiting and retaining this workforce a challenge for many, and is either unknown, or misunderstood by students, and career counselors and parents planning the future for our youth.

To help forge a common set of definitions for the cybersecurity workforce, the interagency *National Initiative on Cybersecurity Education* (NICE), created the *NICE Cybersecurity Workforce Framework* which organizes cybersecurity jobs into specific areas and includes the responsibilities and required skills for each. We must map our offerings to this framework, to ensure the curriculum matches the need, students have a definable career path, and the workforce pipeline is filled. Only through a concerted and coordinated effort, enabled by working sessions such as the CISSE K-12 Cybersecurity Education Summit, can we successfully meet this national challenge.

[6] For more information see http://csrc.nist.gov/nice/index.htm

Agenda
CISSE K-12 Cybersecurity Education Summit
in Partnership with the CISSE K12 Working Group

Facilitator: Davina Pruitt-Mentle, ETPRO/CWK12

Sunday June 10, 2012

12:00 PM – 12:30 PM Welcome / Introductions and Objectives

12:30 PM –1:30 PM (Activity 1)

CISSE Working Group Update Briefs

- Earlier Final Reports
- Standards Overview
- The Role of CTE tracks
- The Role of Competitions
- NICE Strategic Plan
- SFS Efforts

BREAK

1:40 PM –3:00 PM Panel (Activity 2)

K12 Cybersecurity Education Options

Paul Wahnish, Career Technical Education Foundation, Inc.
Skip Lawver – EMU/ Lenawee schools cyber security opportunities
Joseph Cuenco - Science Center of Pinellas County; Cyber Security Education
CyberWatch, (Cybersecurity CTE Path/ Career Academies)
Sheryl Hale, (CTE Path/ Career Academies)
Alec Yasinsac and Les Barnett – AL Computer Science as a Pathway

BREAK

3:00 PM –4:00 PM (Activity 3)

4:00 PM –4:30 PM CISSE Working Group

Mission and Vision

4:30 PM –5:00 PM Closure / Reporting Out / Next Steps

Mission Statement DRAFT

The mission of the CISSE K-12 Working Group (WG-K12) is to be a ***leading resource for K-12 cybersecurity education***. The special interest group serves its members and represents the interests of Cybersecurity education by fostering high quality discussion, dialogue, sharing and promoting professional growth through:

1. Advancement of education and practice,
2. Facilitation of quality research,
3. Professional development of its members, and
4. Encouraging an interaction between the Cybersecurity professional, higher education faculty and K-12 communities

Vision Statement DRAFT

The CISSE K-12 Working Group (WG-K12) is a leading authority in K-12 cybersecurity education. WG-K12 leads through discussion, professional development and dissemination of current information/trends, current practice, research initiatives and outreach programs with Cybersecurity professional, higher education faculty and K-12 communities.