2010

CISSE K-12 Security Initiative Working Group Report

Cybersecurity Workforce Pipeline

June 7-8, 2010 – Baltimore, MD

CISSE

http://cisse.info/

Table of Contents

Introduction

Information technology has moved beyond a luxury solely for the business world. It is an integral part of the modern world forming a central part of everything including communications, commerce, shipping, control of power plants, and entertainment. It is quickly ubiquitous outside the formal classroom setting and is becoming a universal part of the educational 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 Colloquium for Information Systems Security Education (CISSE) or more simply -- *The Colloquium*, was established to provide a forum for dialogue among leading figures in government, industry, and academia. The *Colloquium* recognizes that the protection of information and infrastructures that are used to create, store, process, and communicate information is vital to business continuity and security. The *Colloquium*'s goal is to work together to define current and emerging requirements for information assurance education and to influence and encourage the development and expansion of information assurance curricula, especially at the graduate and undergraduate levels. This is coupled with a growing recognition for the need to increase outreach efforts to both the general citizenry and the K12 educational community.

Citizens need to be aware of general cybersecurity concepts, and a workforce competent in the technical field must be developed. Over time, awareness of Cyber Ethics, Safety and Security (C3) issues has clearly grown. Almost universally, the educational community believes these topics should be taught in schools, and the number of schools with policies that require coverage of this important subject matter has increased. At the same time, the education and training of a skilled and competent Cybersecurity workforce is an essential element in protecting the nation's computer and information systems. While not as mature as C3 awareness programs, there has been an increase in a growing number of efforts to attract, recruit and retain students into the Cybersecurity or related STEM fields. Unfortunately, many of these efforts have occurred within their own silos, and as a result there are few discussions sharing lessons learned and very little cross pollination of ideas.

To examine these issues, the CISSE K-12 Security Initiative Working Group session took place on June 7-8, 2010 during the 14th annual Colloquium for Information Systems Security Education (CISSE) conference in Baltimore, MD. The 40-plus working group participants engaged in discussions to share existing programs, projects and activities, key challenges, promising strategies, and effective progress measures for developing a competent cybersecurity workforce for the digital age. An initial synthesis of the working group session discussion was presented at the conference plenary session on June 8th.

Working Group Discussions

Currently, several K12 Cybersecurity efforts throughout the country are appearing. Unfortunately, there are few opportunities to share programs or collaborate on existing efforts. A K-12 Working Group allowed members throughout the country to come together to share ideas and brainstorm collaborative projects with a common focus: *Cybersecurity Workforce Pipeline*.

The workshop session was attended by CISSE participants representing a wide demographic audience to include K-12 educators and central office staff, Career Technology Education (CTE) educators, department of education personal, two and four year faculty, federal and industry representatives and high school and undergraduates students.

Participants shared current and proposed program efforts, identified key challenges, and explored promising strategies for developing a component cybersecurity workforce. The session addressed three objectives: learning about current K12 cybersecurity curriculum, groups and projects, identifying areas of need, and sharing recommendations for possible best practices and national initiatives.

The session began with information sharing and community building across program disciplines through introductions and interest statements. During the 90 minute first day session participants were asked to share their personal opinions to two key questions:

- *What is Cybersecurity Education?*
- *What are the areas of greatest need for cybersecurity education?*
  - *What is already happening?*
  - *What else needs to be done?*

Two attendees kept notes of the open group discussion. The working group chair, Dr. Davina Pruitt-Mentle, met with note keepers to review and consolidate findings. Key recommendations and findings were summarized and shared on Day 2 during a one hour session. Consensus was obtained regarding findings, and additional input was added after reviewing the content with the K12 working group session participants. Recommendations to address at further working group sessions were collated. The results were reported at a conference plenary closing session.[1]

Cybersecurity Education

What is Cybersecurity Education?

Participants agreed that the term Cybersecurity is problematic. The term is often used by K12 academia and lay persons as an interchangeable term for internet safety. In the career realm, Cybersecurity covers a vast number of job titles and pathways.

Participants identified the need to differentiate between Cybersecurity "awareness" and Cybersecurity education related to workforce development. Several analogies surfaced during the discussion. In schools, students learn about drug, alcohol and HIV awareness. However, while awareness programs in these areas have brought about student content knowledge awareness and studies claim

[1] Session agenda is available in Appendix A.

positive impacts on behavior, these programs do not directly address career awareness in the fields of medicine or pharmacology.

The workgroup identified differences between awareness and education including:

- Cybersecurity awareness often crosses over into general cyberawareness topics and "hot topics" such as sexting and cyberbullying. These hot topics are usually the focus of most common programs.
- Awareness programs focus on skills necessary to keep personal data, identity, and technology safe, while workforce education focuses on the skills necessary to keep everyone's personal data, identity, and technology safe.
- Workforce programs provide a comprehensive look at multiple vulnerabilities with the purpose of prioritizing interventions based on context and budget while awareness efforts are a subset of skills that focus often on the "top 10" or fewer vulnerabilities.
- Cybersecurity awareness programs emphasize personal habits that need to be established while Cybersecurity education programs focus on multiple domains requiring specialized knowledge (e.g. network, IT, IS, Disaster Recovery)

Participants also noted the distinction between technician careers such as networking and system administration versus traditional STEM pathways, such as computer science and engineering, as well as digital forensics through criminal justice departments which are encompassing Cybersecurity. These two distinct groups may need to be addressed through different mechanisms. Traditional STEM pathways need to be explored to reveal what has and has not worked and how a new dimension of Cybersecurity content might impact recruitment and retention. Technical and certification pathways which lead toward workforce opportunities and the accompanying recruitment required for two year and high school levels also needs to be explored. Combining analysis of both traditional and technical identities should focus on the competence and affordability from both the macro and micro perspective.

Participants noted that there are more opportunities for the teaching of awareness than the instruction in cybersecurity technical fields. Several existing programs were shared and it was noted that a growing number of opportunities for cyberdefense competitions were surfacing. More information needs to be shared explaining the profession and defining cybersecurity education in terms of workforce development, and the skills and knowledge required for success. The breadth of the field and the plethora of the career paths make this information critical.

Current Landscape

- *What are the areas of greatest need for cybersecurity education?*
  - *What is already happening?*
  - *What else needs to be done?*

The following provides an overview of programs that were shared by participants that are related to existing cyberawareness efforts.

Programs and Competitions: Awareness

EDUCAUSE Awareness Campaign

The EDUCAUSE/Internet2 Higher Education Information Security Council has compiled, and continues to update, extensive cybersecurity awareness resources and activities from partner colleges and universities. Materials are appropriate for multiple age groups and audiences. Archives to case studies and impact studies are also available.

EDUCAUSE Annual Security Video Contest

Every two years, the EDUCAUSE/Internet2 Higher Education Information Security Council (HEISC) and its partners hold an Information Security Awareness Poster & Video Contest to raise awareness of and increase information security at colleges and universities. These student-created materials are available for use in campus security awareness campaigns during student orientation, National Cyber Security Awareness Month (October), and throughout the year. Visit the Cybersecurity Awareness Resource Library for a compilation of cybersecurity awareness materials for colleges and universities. Most can be used for multiple audiences and age groups.

National Cybersecurity Awareness Campaign Challenge

The Awareness Challenge is a contest to solicit ideas from individuals and industry about how to best engage the American public in a discussion about cybersecurity. Proposals were submitted to DHS and were evaluated based on factors that included teamwork, effective metrics for distribution and engagement, use of Web 2.0 technology, compliance with spam laws, privacy, repeatability, feedback mechanisms, list building, transparency, and message. Winners have the opportunity to help plan the National Cybersecurity Awareness Campaign with DHS and to prepare the campaign for its launch in October, during Cybersecurity Awareness Month. It is not clear if this will be an annual event.
http://www.dhs.gov/files/cyber-awareness-campaign.shtm

National Cyber Security Division, DHS

The National Cyber Security Division outlines the Department's strategic national cybersecurity objectives. NCSD works collaboratively with public, private and international entities to secure cyberspace and America's cyber assets. Examples of current cyber preparedness and response programs include: Cybersecurity Preparedness and the National Cyber Alert System, US-CERT Operations, National Cyber Response Coordination Group, and the Cyber Cop Portal. Through Cyber Risk Management, the National Cyber Security Division seeks to assess risk, prioritize resources, and execute protective measures critical to securing our cyber infrastructure. Examples of current cyber risk management programs include: Cyber Exercises: Cyber Storm, National Cybersecurity Awareness Month, and the Software Assurance Program.

US-CERT

The U.S. Computer Emergency Readiness Team (US-CERT) offers safety tips, incident reports, and the latest cyber alerts.

National Cyber Security Alliance

The National Cyber Security Alliance (NCSA) is a collaborative effort among experts to provide free tips, checklists, and best practices for remaining safe while online.

MS-ISAC

The Multi-State Information Sharing and Analysis Center (MS-ISAC) comprises members of all 50 states, local governments, and U.S. territories and districts, and provides downloadable awareness materials including newsletters, posters, bookmarks, and briefings. They also conducted a national Kindergarten through 12th grade Computer Safety Contest, to encourage young people to use the Internet safely and securely and to craft messages and images that will best resonate with their peers across the country to stay safe online. http://www.msisac.org/awareness/poster2010/index.cfm

Federal Trade Commission

The Federal Trade Commission's OnGuard Online Web site provides practical tips and downloadable print and Web materials about how to avoid Internet fraud and how to protect personal information. The Net Cetera Community Outreach Toolkit helps provide the community with information about protecting kids online. Resources are being used widely in the K12 arena.

NYUPoly Security Awareness Video Competition

NYUPoly hosts a competition open to high school, undergraduate, and graduate students located in the U.S. Entries submit a "public service" video or animated spot aimed at raising awareness of everyday cyber security. http://www.poly.edu/csaw2011/csaw-awareness

ETPRO/CyberWatch K12

Educational Technology Policy, Research and Outreach (ETPRO) leads the CyberWatch K12 Division efforts. ETPRO is a research and development organization headquartered in Maryland that connects educational technology policy and research to instructional practice. ETPRO originated from the Educational Technology Outreach division of the College of Education, at the University of Maryland, and in 2007 was founded as an entrepreneurial entity committed to quality education for all learners, targeting the effective use of cutting edge technology in formal and informal educational settings to increase interest in Science, Technology, Engineering and Mathematics (STEM) fields. The fundamental gap between technology use and understanding of proper practices, lead ETPRO to the forefront of research, program evaluation and development of Cyberethics, Cybersafety, and Cybersecurity (C3) initiatives. The holistic C3 policy framework has been adopted by Internet Safety

curriculum providers, state and local education entities and state attorney general offices. Adopting a policy framework adds the potential to broaden the impact on students, teachers, and parents in addressing ALL areas determined by government, business and industry, health agencies, and education to be of increasing importance. The STEPP scaffold allows schools to apply the C3 framework within their school's improvement plan. ETPRO has also launched the C3 Schools initiative, similar to a Green School Program. Other research efforts that may be of interest include:

- National C3 Baseline Study
- 2010 C3 Follow Up Survey
- Research Priorities in Cyberethics, Cybersafety and CyberSecurity : A Delphi Study
- Priorities in CyberSecurity Education : A Delphi Study
- MD Information Literacy, Ethical Use and Academic Integrity Baseline Pilot Study
- Review of Research: The Status of Cyberawareness in US Schools
- Effects of C3 Curriculum Integration on Attitudes of Teachers and Students
- Students' Perceptions of Internet Safety Modules
- School-Based Staff Development for Teaching Cyberethics, Safety and Security Curriculum
- Gender Differences in Student Attitudes Toward Internet Safety Curriculum

http://www.edtechpolicy.org/cyberk12/c3awareness.html

Internet Safety Providers (ISP)

Numerous Internet Safety Providers provide resources and tools, professional development opportunities and community outreach. The list below is an inventory compiled from the resources shared in discussions over the two day working group sessions.

ISP	Website
iKeepSafe	http://www.ikeepsafe.org/
WebWise Kids	http://www.webwisekids.org/
Get Net Wise	http://kids.getnetwise.org/tools/
iSAFE	http://www.isafe.org/
NetSmartz	http://www.netsmartz.org/
CommonSenseMedia	http://cybersmartcurriculum.org/
CyberSmart!	http://cybersmart.org/
WoogiWorld	http://www.woogiworld.com/
MS Digital Citizenship	http://digitalcitizenshiped.com/Default.aspx
SAFE-Net	https://safenet.3rox.net/
Digital Citizenship and Creative Content	http://www.digitalcitizenshiped.com/
NCSA	http://www.staysafeonline.org/
CCIP	http://www.cybercrime.gov/cyberethics.htm

ISP	Website
(ISC)2	https://cyberexchange.isc2.org/safe-secure.aspx
Garfield	http://learninglab.org/
BrainPop	http://www.brainpop.com/technology/computersandinternet/onlinesafety/preview.wem
CLICKS	http://www.oag.state.md.us/clicks.htm
NDAA	https://www.thecjportal.org/ICAC/Courses/Pages/NDAA.aspx
Google Digital Literacy Tour	http://www.google.com/educators/digitalliteracy.html

Most schools and school districts have developed content to use with their students, educators and parents. These are often based on what their partner ISP has already developed and they either use it as written or extend it with their own materials folded in. More schools have begun to develop cyber education materials, often called Internet Safety Curriculum as a result of the Federal Communications Commission's recent release of an order that will require schools to educate students about Internet safety in order to comply with the federal E-Rate program, which provides funding for schools to achieve online connectivity. The requirement comes from language in the Protecting Children in the 21st Century Act, which was signed into law as a part of the Broadband Data Improvement Act in October 2008.

The measure will require schools to provide education about appropriate online behavior in chat rooms and on social-networking websites, as well as information about cyberbullying. It does not stipulate what kinds of curricula or procedures this may entail, nor does it define "cyberbullying" or "social networking," although it does mention several resources that schools may refer to for further explanation. Schools are required to update their Internet safety policies to reflect this change by July 1, 2012.

Below is a partial list of states' content related to cyber awareness.

AL	http://alex.state.al.us/standardAll.php?subject=TC2&summary=1 http://alex.state.al.us/podcast_view.php?podcast_id=756
AK	http://www.eed.state.ak.us/standards/pdf/standards.pdf
AR	http://www.arkansassafeschools.org/ http://www.dawson.dsc.k12.ar.us/DepartmentsPrograms/TechnologyIntegration/InternetSafetySecurity/tabid/135/Default.aspx http://www.arsafeschools.com/Training/Training110718.asp
AZ	https://sites.google.com/a/lesd.k12.az.us/lesdinternetsafety/parent-resources
CA	http://ecitizenship.csla.net/2011/02/module-1-what-is-digital-citizenship.html http://pubs.cde.ca.gov/tcsii/ch8/internetsafety.aspx
CO	http://safeschools.state.co.us/Resources2.html http://safeschools.state.co.us/other_resources.html
CT	http://healthsciencetechnology.wikispaces.com/Digital+Citizenship http://www.sde.ct.gov/sde/cwp/view.asp?a=2618&q=321096
DC	
DE	http://www.doe.k12.de.us/infosuites/students_family/climate/ http://dti.delaware.gov/
FL	http://www.fldoe.org/safeschools/internetsafety.asp http://www.fldoe.org/safeschools/bullying.asp
GA	http://www.gaicac.us/Modules/CybersafetyRisks.pdf
HA	http://doe.k12.hi.us/technology/index_internet.htm http://atr.k12.hi.us/internet_safety.html
IA	http://educateiowa.gov/index.php?option=com_content&view=article&id=2484:grades-9-12&catid=1128:iowa-core-21st-century-skills&Itemid=4600
ID	http://idahochildrenstrustfund.state.id.us/publications/ICTF_Spring_06_rev.pdf http://www.sde.idaho.gov/schoollibraries/docs/tech/slim.pdf http://www.sde.idaho.gov/site/postleg/docs/2011/Senate%20Bill%201184/1184%20Technology%20Supporting%20Docs/Sample_Tiered_Tech_Use_In_Classrooms_Washington_State_2010.pdf http://www.sde.idaho.gov/site/content_standards/infoCommTechStandards.htm
IL	http://www.isbe.state.il.us/curriculum/html/internet_safety.htm
IN	http://mustang.doe.state.in.us/dg/olt/netsafety/search.cfm
KS	http://www.ksde.org/Default.aspx?tabid=3909
KY	http://www.kysafeschools.org/internetsaf.html
LA	http://region2internetsafety.pbworks.com/w/page/28122179/Internet%20Safety%20in%20the%20Classroom
MA	http://www.doe.mass.edu/news/news.aspx?id=1100 http://www.doe.mass.edu/bullying/ http://www.doe.mass.edu/edtech/standards/itstand.pdf http://www.mass.gov/?pageID=berterminal&L=2&L0=Home&L1=Community+Outreach+%26+Education&sid=Dber&b=terminalcontent&f=conferences_educational_initiatives&csid=Dber
MD	http://www.msde.maryland.gov/MSDE/programs/technology/ http://www.bcpl.info/info/parenting/#internet http://www.marylandpublicschools.org/msde/programs/technology/library_media
ME	http://www.maine.gov/mlti/csm/index.shtml http://www.maine.gov/ag/children_families/internet_exploitation.html
MI	http://www.oakland.k12.mi.us/Departments/GovernmentCommunityServices/OfficeofSafeSchools/tabid/656/Default.aspx http://www.michigan.gov/cybersecurity http://www.michigan.gov/ag/0,1607,7-164-17334_48889---,00.html
MN	http://www.informns.k12.mn.us/Internet_Safety.html http://education.state.mn.us/MDE/Learning_Support/School_Technology/index.html
MO	http://www.mo.gov/living-in-missouri/internet-safety/
MS	http://www.jackson.k12.ms.us/content.aspx?url=/page/709

	http://www.mde.k12.ms.us/ACAD/ID/Curriculum/Curr.htm
MT	http://opi.mt.gov/Resources/InternetSafety/index.html
NC	http://www.ncpublicschools.org/docs/acre/standards/new-standards/info-technology/gradek.pdf
ND	http://www.dpi.state.nd.us/standard/content/tech_draft2011.pdf
NE	http://www.education.nh.gov/instruction/curriculum/tech/documents/guide.pdf
NH	http://www.nheon.org/oet/safety.htm http://www.education.nh.gov/safety.htm
NJ	http://www.state.nj.us/education/schools/security/links/isb.htm
NM	http://www.ped.state.nm.us/searchResults.html?cx=005504269637186596122%3A1bb6hgx7phu&cof=FORID%3A11&q=internet+safety&sa=Search#967
NV	http://nde.doe.nv.gov/EmployeeResources.htm
NY	http://www.p12.nysed.gov/technology/internet_safety/resources.html http://www.p12.nysed.gov/technology/internet_safety/
OH	http://www.ode.state.oh.us/GD/Templates/Pages/ODE/ODEPrimary.aspx?page=2&TopicRelationID=1714 http://www.infohio.org/parent/
OK	http://www.netsmartz.org/Overview/StatePartnerships
OR	http://www.ode.state.or.us/search/results/?id=141
PA	http://www.attorneygeneral.gov/kidsparents.aspx?id=1559
RI	http://www.ride.ri.gov/instruction/curriculum/rhodeisland/roles/familyweb.aspx
SC	http://csafety.scaet.org/SC_Internet%20Safety%20Standards_K-12.pdf
SD	http://library.sd.gov/LIB/SLC/SDSL-SchoolLibContentStandards-DRAFT.pdf
TN	http://www.tn.gov/education/cte/standardscurr/te_1011.shtml
TX	http://www.txssc.txstate.edu/K12/
UT	http://www.schools.utah.gov/charterschools/Training/Directors-Meetings/2011-Directors-Meetings/October-2011/Internet-Safety-Training.aspx http://www.netsafeutah.org/
VA	http://www.doe.virginia.gov/support/safety_crisis_management/internet_safety/guidelines_resources.pdf
VT	http://education.vermont.gov/new/html/pgm_edtech/resources.html
WA	http://www.atg.wa.gov/YISTF.aspx
WI	http://www.k12.wa.us/edtech/InternetSafety/default.aspx
WV	http://www.verizonreads.net/about/press/newstory_verizon_intrnet_safty09.shtml http://wvde.state.wv.us/technology/tutorials/
WY	http://edu.wyoming.gov/searchresults.aspx?SearchQuery=internet+safety

In addition to the information about cybersecurity awareness, the group shared programs related to cybersecurity career awareness.

Programs and Competitions: Cybersecurity Career Awareness

US Cyber Challenge

Cyber Security Treasure Hunt and Cyber Camps

Cyber Security Treasure Hunt targets adults and college students and very talented high school students who want to prove they have basic mastery of vulnerabilities and other areas of security. Like a scavenger hunt, the contest delivers online quiz components that send candidates to a simulated environment where they can safely explore, find answers and return to the quiz. This is the primary qualification for students to earn a place in the cyber camps.
http://www.uscyberchallenge.org/

CyberPatriot

CyberPatriot targets high school students who harden systems to block attacks and are scored on their success in keeping the

attackers out.
http://www.uscyberpatriot.org/Pages/default.aspx

NetWars

NetWars targets adults and college students and very talented high school students who have very high levels of skills and want to prove they should win internships and scholarships at important organizations. Students work in real-world, online laboratories where contestants must capture and hold cyber territory as hundreds of others try to do the same.
http://www.sans.org/cyber-ranges/netwars/#upcoming

DC3 Digital Forensics Challenge

The DC3 Digital Forensics Challenge offers separate competitions for high school, undergraduates and adults to show their forensics skills. Data is presented from actual cases investigated by the DOD Cyber Crime Center and asks four levels of questions. The forth level includes questions even DC3 does not know how to answer.
www.dc3.mil/challenge/

NetRiders

NetRiders is an annual competition organized by the Cisco Systems to provide exposure to the network academy students as they progress towards the ICT workforce.
http://www.cisco.com/web/learning/netacad/us-can/netriders.html

CSAW Cybersecurity Competition at NYU-Poly

A number of activities including:

High School Cyber Forensics Challenge

Students discover the fascinating world of cybersecurity such as log and file analysis, rootkit detection and analysis, botnet detection and analysis, live system forensics, steganography and file carving. School's teams battle against other elite teams – and the clock – as they solve this fast-paced mystery. The challenge takes place remotely over the Internet. Twelve teams of finalists are brought to NYC with their faculty mentors to compete in the finals competition and awards ceremony. The cost of the trip is covered by the competition.

The CSAW Capture the Flag Competition

Contest designed to evaluate application security skills. Competitors attack vulnerable applications and solve offensive challenges. Challenges are divided into technical categories and assigned point values based on how difficult they are. The CSAW CTF is loosely based on the widely known DEFCON Capture the Flag competition.

Embedded Systems Challenge

The annual Embedded Systems Challenge (ESC) focuses on the red-team/blue- team approach to assessing the trustworthiness of hardware. Teams are invited to participate in this challenge and attack a target hardware platform. They discover vulnerabilities in the target platform and exploit them by using their hardware design skills.

The Quiz Tournament

The Quiz Tournament tests the breadth and depth of knowledge in broad range of digital security topics. The covered topics include, but are not limited to, network security,

cryptography, malware, application and web security, protocols, the history of digital security, digital forensics, and policy, risk management, and standards.

Kaspersky's American Cup

Kaspersky's American Cup is an inspirational conference that brings together students, experts, scientists and researchers in a collaborative environment to present and discuss issues relating to cybercrime. To participate in the conference and Kaspersky's American Cup at NYU-Poly CSAW, potential attendees must submit research on the topic of "Cyber Security" via the Kaspersky site. Selected authors are invited to attend the conference and are automatically entered in the challenge and asked to present their papers.

DEF CON

An entire weekend of non-stop online security challenges that test everything from simple trivia to advanced reverse engineering and exploit development. Contestants are faced with a with a variety of topics including Pursuits Trivial, Crypto Badness, Packet Madness, Binary L33tness, Pwtent Pwnables, and Forensics. There were point values ranging from 100 to 500, with increasing levels of difficulty for the increased point value. Quals go on to compete in Las Vegas during Defcon against the previous year's winning team.
http://www.defcon.org/Cyber Defense Exercises

National Collegiate Cyber Defense Competition

CCDC is a three day event and the first competition that specifically focuses on the operational aspect of managing and protecting an existing "commercial" network infrastructure. Not only do students get a chance to test their knowledge in an operational environment, they will also get a chance to network with industry professionals who are always on the look out for up and coming engineers. CCDC provides a unique opportunity for students and industry professionals to interact and discuss many of the security and operational challenges the students will soon face as they enter the job market. http://www.nationalccdc.org/

CyberWatch K12 Mindtools and CyberSTEM™ Programs

Programs are offered at the elementary, middle and high school level. Programs are offered before, after and within school as extension programs or through supplementary lessons/units infused into core content. In addition, summer camps are offered targeting middle and high school students. CWK12 works in partnership with State Departments of Education and higher education institutions to offer a high school Cybersecurity CTE track.

The underlying theme of the CyberSTEM content is to *foster excellence in 21st century skills and digital literacy (technology fluency and applications, team building, collaboration tools, problem based critical thinking), which helps students succeed in college, and prepare themselves with the skills necessary to meet the shifting and constantly changing demands of the future workplace.*

Member institutional partner programs (both two and four year) are housed in a variety of departments/schools. Thus, content introduces students, educators and parents to a plethora of career pathways to include computer science, business, mathematics, engineering, criminal justice, psychology, information assurance, networking, information technology etc. Five module "topics" have been developed in collaboration with partner IHE's to meet their specific needs. Students learn about programming/computational logic, coding-decoding/cryptography, system vulnerabilities, digital forensics and careers in information assurance/cybersecurity, as well as learning more about the security clearance processes and identity management strategies.

CyberWatch K12 SECURE IT™: Strategies to Encourage Careers in CyberSecurity and IT

The *SECURE IT* model design is comprised of seven essential components: after-school and Saturday programs for elementary and middle school students; summer programs for high school students; teacher professional development; training and materials for counselors and STEM coordinators; integrated core curricular modules; resources and activities for parents/guardians, and a new Cybersecurity Olympiad competition.

Wilmington University

Wilmington sponsors several area high schools in preparation for the US Cyber Foundations competition.

Key Points

Common Threads: Awareness

Participants agreed there is a distinct difference between general cyberawareness education content and career readiness content for the field of Cybersecurity. Participants agreed that all stakeholders have a responsibility for advancing the cyber awareness endeavor. Essential components for a cyberawarness program should include:

- A National Tag Line
- An on-going National Media Campaign
- Content and media that impacts multiple change agents; parents, educators (many educators are also parents), students, and also includes SIO's, law enforcement, etc.
- Efforts directed towards students should
    - Use positive messaging
    - Use media – e.g., YouTube
    - Perhaps include students teaching students (NOTE: research shows students indicate parental input key and student must learn how to train before they train others)
    - Perhaps include gaming/online modules—"Slay the malware"
- Efforts directed all stakeholders should
    - Include hands-on activities and how to's
    - Focus moving away from "put online and they will come"

There was discussion regarding whether or not there is a need for a separate set of Cybersecurity standards to accompany existing standards. The working group shared options including the development of a separate curriculum which could become stand alone content or could be folded into existing technology credit and content already

covered in existing standards. Many of the higher education community were not as well versed in the current sets of K12 standards to include, technology, educational technology, computer science, engineering, digital literacy, media literacy and 21st Century Skills. It was noted that a variety of barriers exist to adding new curriculum and standards. These include:

  - Already packed curriculum
  - Lack of funding
  - Need for professional development
  - Competition with other stakeholder groups

The K12 participants did share there is a disconnect between what is already taking place in K12 and many stakeholder perceptions. For example, the notion that no training or teaching related to these topics is taking place in K12, in spite of the fact that there are several sets of standards in existences which are addressing many issues. K12 attendees also noted curriculum focus is already shifting within many ISPs to include Cybersecurity and the connection with other STEM competencies.

Recommendations: Awareness

- Participants desired one central archive for materials, so members can visit and see what has already been created, and what has been implemented successfully. Many people were already aware of the EDUCAUSE repository and would like to see something similar done for K12.
- It was agreed that there needed to be more communication between K12, higher education and industry. Each group was doing things individually, and there was virtually no evaluation of impact and in many cases a disconnect takes place between what works in K12, what works on campus and what works in industry.
- More research is needed on what works and what schools are doing to address cyberawareness.

Common Threads: Workforce

Items noted by participants include:

- Many interesting programs happening and there is a need to share so others can replicate
- Growing focus on cyber defense competitions and activities, but it was noted that not all students are attracted to these types of activities and little training is provided for educators to lead the efforts
- Limited programs that focus on attracting students to other areas of Cybersecurity
- There is a need to attract underrepresented groups
- Many were unsure about what technology is being taught in schools

Stakeholders do not understand what is taking place in K12. For example, they do not have knowledge of what is being taught in school technology courses, what STEM research has already been done, what other groups have done in recruiting and retaining students in STEM fields such as computer science and engineering, and what standards are already in place.

Recommendations: Workforce

- Participants desired one central archive for materials, so members can visit and

see what has already been created, and what has been implemented successfully.

- Lines of communication between K12, higher education, and industry need to be opened to expand replication, share knowledge of best practices, and perform better evaluation of impact. Similar to cyber awareness programs, there is a disconnect between what works in K12, in higher education and what works in industry.
- More marketing of STEM careers on social media.
- Professional development for all faculty.
- A research review of existing standards to prepare students for higher education and cybersecurity workforce pathways is required.
- The requirements both in terms of courses and skills for the possible Cybersecurity career pathways need to be delineated.
- Outreach to parents, students and other stakeholders regarding career options and pathways need to be expanded.
- A list of existing programs with degrees and certifications in Cybersecurity is needed. Many are not advertised as Cybersecurity. Differences between technician Cybersecurity and Computer Science/Engineering Cybersecurity careers need to be explained.
- Stronger articulation between K12, 2 year, and 4 year institutions is needed.

Conclusion: A K12 Working Group

Participants agreed that all stakeholders have a responsibility for advancing the cyber security endeavor. Essential components focus on both cyberawareness and career development. All participants want high quality STEM programs with tracts leading to the plethora of career options in Cybersecurity. They recognize the roles of both technical and traditional STEM pathways in meeting the Cybersecurity workforce need. The working group understands that these different trajectories may require different strategies but have similar end goals.

On-going forums, like the CISSE K-12 Working Group, will provide a means to foster dialogue among leading figures in government, industry, and academia to define current and emerging requirements for information assurance education and to influence and encourage the development and expansion of information assurance curricula, not just in higher education, but in K12 as well. The Working Group session generated enthusiasm for future dialogues, conversations, and joint activities to benefit STEM education students, educators, and the nation.

Appendix A: Agenda

K-12 Security Initiative Working Group

Currently, several K12 Cybersecurity efforts throughout the country are starting to appear. Unfortunately, there are few possibilities to share programs or collaborate on existing efforts. A K-12 Working Group will allow members throughout the country to come together to share ideas and brainstorm collaborative projects with a common focus: Create a Competent Cybersecurity Workforce for the Digital Age.

Our working group sessions are designed to meet four objectives:

(1) learning about other K12 Cybersecurity curriculum, groups and projects,

(2) fostering cross-site collaboration of K12 Cybersecurity stakeholders, and

(3) synthesizing and publishing existing projects and resources, and

(4) networking with other agencies and resources.

Desired Outcomes

By the end of the sessions participants will have:

- A better understanding regarding the definition of Cybersecurity education
- Received updates RE existing programs, projects and activities (or those in development)
- Developed outline of current programs and gap analysis (if any)
- Developed consensus regarding recommendations for possible best practices or local and national initiatives
- Identified and finalized recommendations for the CISSE Working Group Report

Tentative Agenda- Day 1

- Welcome
- Overview of Working Group Objectives
- Introductions

- Discuss working group objectives identify targets/strategies for the group to address
- Sharing of program activities and ideas
- Small group – What's the Big Idea—How do we get there
- Debriefing / Synthesize today's ideas
- Next steps for Day 2

Reports

- Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group (OSTWG) http://www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf
- National Crime Prevention Council: "Protecting Teens from Identity Theft" (http://www.ncpc.org/programs/teens-crime-and-the-community/publications-1/preventing-theft/adult_teen%20id%20theft.pdf)
- 24 Yale Alumni Magazine: "A Closer Look at Alcohol" (http://www.yalealumnimagazine.com/issues/01_05/alcohol.html)
- "The State of Cyberethics, Cybersafety, and Cybersecurity Curriculum in the US": Survey (http://www.staysafeonline.org/content/ncsa%E2%80%99s-national-k-12-studies)
- "Children and the Internet: Laws Related to Filtering, Blocking and Usage Policies in Schools and Libraries" (http://www.ncsl.org/issuesresearch/telecommunicationsinformationtechnology/stateinternetfilteringlaws/tabid/13491/default.aspx)
- Net Cetera: Chatting With Kids About Being Online (http://www.onguardonline.gov/topics/net-cetera.aspx)
- National Education Technology Plan 2010, US Department of Education (http://www.ed.gov/technology/netp-2010)
- President Obama, in his Cyberspace Policy Review released on May 29, 2009, recommended that the United States initiate a K-12 cybersecurity education program for digital safety, ethics, and security and develop a public awareness campaign.
- "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure" (http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)
- Full report National C3 Baseline Study http://staysafeonline.mediaroom.com/index.php?s=67 (ETPRO)

Appendix B: ISTE NETS*S Standards

National Educational Technology Standards (NETS*S)and Performance Indicators for Students

1. Creativity and Innovation

Students demonstrate creative thinking, construct knowledge, and develop innovative products and processes using technology. Students:

a. apply existing knowledge to generate new ideas, products, or processes.
b. create original works as a means of personal or group expression.
c. use models and simulations to explore complex systems and issues.
d. identify trends and forecast possibilities.

2. Communication and Collaboration

Students use digital media and environments to communicate and work collaboratively, including at a distance, to support individual learning and contribute to the learning of others. Students:

a. interact, collaborate, and publish with peers, experts, or others employing a variety of digital environments and media.
b. communicate information and ideas effectively to multiple audiences using a variety of media and formats.
c. develop cultural understanding and global awareness by engaging with learners of other cultures.
d. contribute to project teams to produce original works or solve problems.

3. Research and Information Fluency

Students apply digital tools to gather, evaluate, and use information. Students:

a. plan strategies to guide inquiry.
b. locate, organize, analyze, evaluate, synthesize, and ethically use information from a variety of sources and media.
c. evaluate and select information sources and digital tools based on the appropriateness to specific tasks.
d. process data and report results.

4. Critical Thinking, Problem Solving, and Decision Making

Students use critical thinking skills to plan and conduct research, manage projects, solve problems, and make informed decisions using appropriate digital tools and resources. Students:

a. identify and define authentic problems and significant questions for investigation.
b. plan and manage activities to develop a solution or complete a project.
c. collect and analyze data to identify solutions and/or make informed decisions.
d. use multiple processes and diverse perspectives to explore alternative solutions.

5. Digital Citizenship

Students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior. Students:

a. advocate and practice safe, legal, and responsible use of information and technology.
b. exhibit a positive attitude toward using technology that supports collaboration, learning, and productivity.
c. demonstrate personal responsibility for lifelong learning.
d. exhibit leadership for digital citizenship.

6. Technology Operations and Concepts

Students demonstrate a sound understanding of technology concepts, systems, and operations. Students:

a. understand and use technology systems.
b. select and use applications effectively and productively.
c. troubleshoot systems and applications.
d. transfer current knowledge to learning of new technologies.

https://www.iste.org/Content/NavigationMenu/NETS/ForStudents/2007Standards/NETS_for_Students_2007_Standards.pdf