UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Formerly UMUC

First State of Maryland GenCyber Teacher Camp Successes

Dr. Brandie Shatto Chair, MEd Instructional Technology, Acting Chair, MAT

Dr. Loyce Best Pailen, CISSP Director Center for Security Studies,

Tuesday, Dec. 10, 2019 - 11:15 am - 11:55 am
Track 1: Increasing Career Awareness – Garden 1

First State of Maryland GenCyber Teacher Camp Successes

Panel 2019 UMGC GenCyber Teacher Participants

Robin Burns
North Point High School
Charles County Public Schools
Cyber Security Teacher

Helene A. Johnson
Cyber Security Teacher
Suitland High School
Prince George's County, Maryland

Lorraine Lloyd
Cybersecurity Teacher
Loudoun Valley High School
Loudoun County, VA

Ken Nwocha
Math Teacher
Montgomery County Public Schools, MD

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Cybersecurity Reality

- General Citizenry – lacks education in cybersecurity
- Top Leadership – lack cybersecurity awareness
- Shortage of Cybersecurity Professionals
- Many teachers, children and students: still lack digital literacy
- Workforce needs not being met or addressed properly

Cybersecurity Supply/Demand Heat Map

All Data | Public Sector Data | Private Sector Data

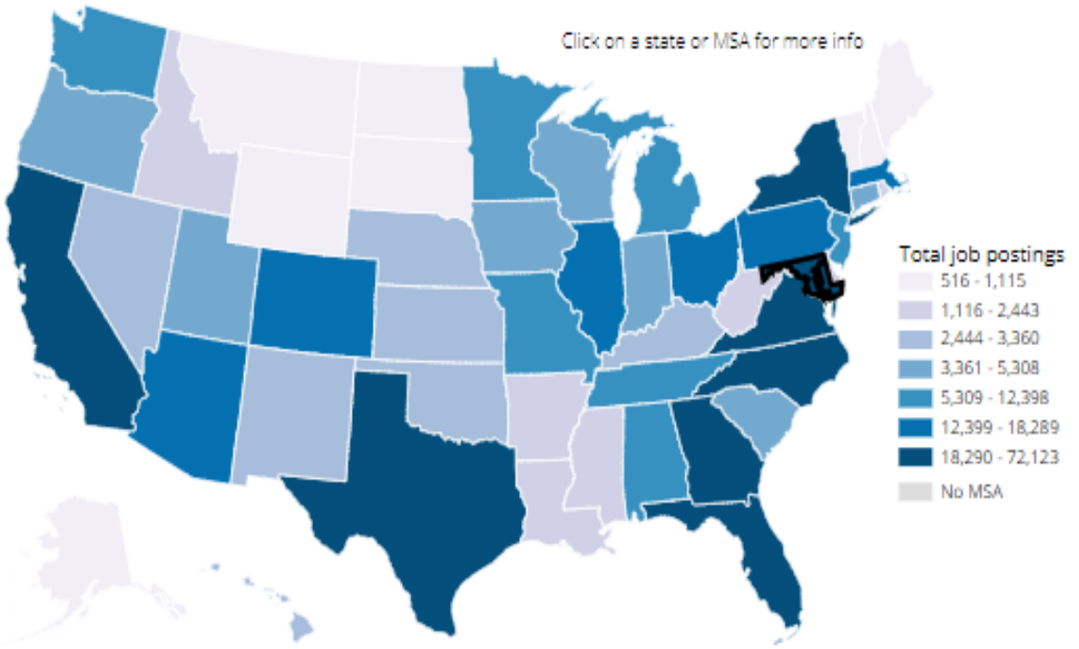
States | Metro Areas

Total job openings

Search State

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your lo rce.

Share | Embed



Maryland

TOTAL CYBERSECURITY JOB OPENINGS

20,516

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

45,412

SUPPLY OF CYBERSECURITY WORKERS

Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO

MD 2.2

National average 2.0

GEOGRAPHIC CONCENTRATION

Very High

LOCATION QUOTIENT

MD 2.7

National average 1.0

TOP CYBERSECURITY JOB TITLES

- Cyber Security Engineer
- Cyber Security Analyst
- Systems Engineer
- Cyber Security Manager / Administrator
- Network Engineer / Architect
- Software Developer / Engineer
- Cyber Security Consultant
- Cyber Security Specialist / Technician
- Systems Administrator

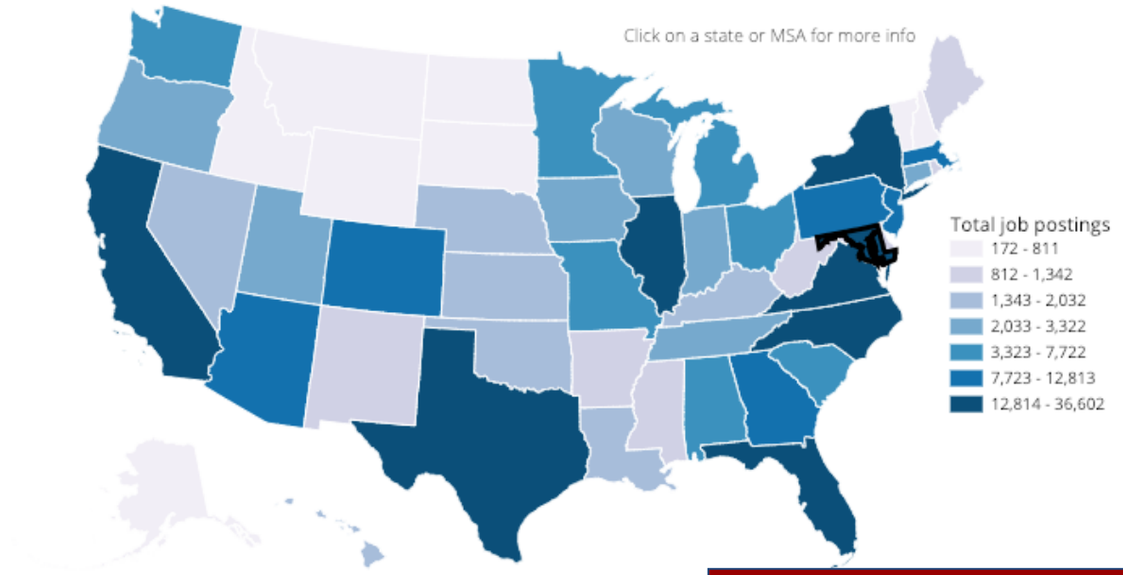
Cybersecurity Supply/Demand Heat Map

All Data | Public Sector Data | Private Sector Data

States | Metro Areas | Total job openings | Search State

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

Share | Embed

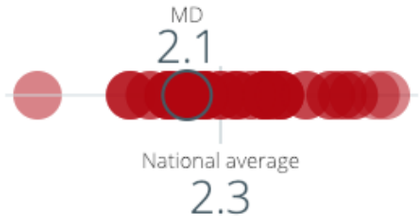


Maryland

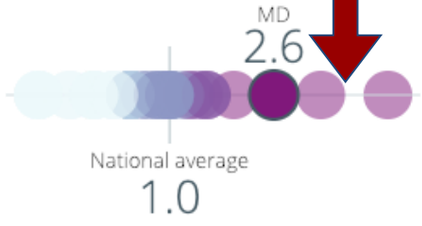
TOTAL CYBERSECURITY JOB OPENINGS
15,128

TOTAL EMPLOYED CYBERSECURITY WORKFORCE
31,386

SUPPLY OF CYBERSECURITY WORKERS
Very Low
CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO



GEOGRAPHIC CONCENTRATION
Very High
LOCATION QUOTIENT



TOP CYBERSECURITY JOB TITLES

- Cyber Security Engineer
- Cyber Security Analyst
- Network Engineer / Architect
- Cyber Security Manager / Administrator
- Systems Administrator
- Systems Engineer
- Software Developer / Engineer
- Cyber Security Specialist / Technician
- Information Assurance Engineer / Analyst

https://www.cyberseek.org/heatmap.html

Please note: VA and DC are both in even greater need with an even lower supply.

Total open jobs:

~60K jobs in cyber in VA/MD/DC

GenCyber Program

- NSA Grants awarded to Institutions to hold GenCyber Summer Camps
- Camp curriculum: increase interest in cybersecurity/teach cybersecurity first principles
- Camp Types: K-12 Student, Teacher or Combination
- Camp Duration – 1-2 weeks, residential/non-residential
- Computer background not required
- Provided at NO cost to the participants

Background – UMGC GenCyber Camp

- The UMGC GenCyber Teacher Camp held July 8-12, 2019 in Largo, MD. (first Maryland Teacher Camp)
- Goals
  - to help High School teachers provide students with a basic understanding of cybersecurity so that they can appreciate how cybersecurity impacts all aspects of their lives. Was
  - designed to promote best practices in cybersecurity pedagogy across content areas and development of curricula, labs . and
  - lesson plans that can be used to infuse cybersecurity principles across many subject areas.
- Attendees: 25 highly qualified High School teachers from the disciplines of
  - Computer Science,
  - Network Technology,
  - Business,
  - Library Science,
  - Math,
- Outcomes
  - Plethora of Lesson Plans
  - Cyber Games
  - Cyber Labs
  - Curricula
  - Supporting tools and technologies

GenCyber Concepts & Goals

Goals

To increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation

To help all students understand correct and safe on-line behavior and how they can be good digital citizens

To improve teaching methods for delivery of cybersecurity content in K-12 curricula

Concepts

- Think Like An Adversary
- Depth Of Defense
- Confidentiality
- Integrity
- Availability
- Keep It Simple

The 6 Cyber Concepts – Think Like an Adversary

- The strategy of putting yourself inside the mindset of a potential attacker that allows you to anticipate attack strategies and defend your systems accordingly.

  - ❖ In order to best protect a student's data, it is useful to think of potential adversaries and their motivations, such as a student wishing harm on another, a student seeking to modify his own data, and consider possible strategies – breaking physically into an office, breaching a network to obtain unauthorized access, etc. and build your security strategy accordingly.

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

The 6 Cyber Concepts – Defense in Depth

- A comprehensive strategy of implementing multiple layers of security tools and techniques within a system so that if one layer fails, another layer of security is already in place to stop the attack/unauthorized access.

  - A castle is secured by a moat, a drawbridge and guards at the gate.
  - Your home computer is secured by locks on the door, an alarm system, and a firewall.
  - Company data is secured by a firewall, passwords, and encryption.

The 6 Cyber Concepts – Confidentiality

- The property that information is not disclosed to individuals, devices, or processes unless they have been authorized to access the information.

  - Student grades can only be accessed by specific individuals within the organization, such as authorized teachers and the principal.
  - At a hospital, medical information about a patient is protected and only provided to authorized personnel.
  - Salary information is typically only available to authorized personnel within a company, such as the supervisor and human resources.

The 6 Cyber Concepts – Integrity

- The property that information, an information system, or a component of a system has not been modified or destroyed in an unauthorized manner.

  - Student grades are accurate and have not been modified by an unauthorized user.
  - A website is the entity it claims to be.
  - A computer system is virus-free and uncompromised.

The 6 Cyber Concepts – Availability

- The property that information or information systems are accessible and usable upon demand.

  - ❖ A student's grades can be viewed by the student and principal and modified by the teacher.
  - ❖ A website for a store is allowing orders to be placed and viewed.
  - ❖ A banking system is appropriately accessible by both customers and banking employees.
  - ❖ A Denial of Service attack can result in a system being unavailable and inaccessible.

The 6 Cyber Concepts – Keep it Simple

- The strategy of designing information and security systems to be configured and operated as simply as possible; all systems perform best when they have simple designs rather than complex ones.

  - ❖ A complex alarm system can have many points of failure, including the hardware and the software.
  - ❖ A complex computer system has many points of access and may be difficult to secure. A simple solution is often the best strategy.

Sub-set of GenCyber Principles /Concepts of Cybersecurity from GenCyber Overview

NATIONAL CRYPTOLOGIC MUSEUM FOUNDATION

A PUBLIC-PRIVATE PARTNERSHIP WITH UNPARALLELED CYBER DEFENSE EXPERTISE.

Code Cracking

Cryptography

Hands-on Hacker Lab

CanaKit

Raspberry Pi 3 model

"Cryptography and Raspberry Pi technology understanding, and implementation will better aid our students towards applying and securing high-paying technology jobs." Helene Johnson PGCPS

There are many ways to define cybersecurity education.

Range from specific to a multi-disciplinary approach.

Elementary

Understanding how computers work and communicate should start in elementary

Encryption and code-breaking throughout K-12

Understanding PII, digital hygiene and citizenship should be a foundational literacy for ALL.

Middle School

Ethics, impact, policy and legal issues may be incorporated into social studies.

Essential technology vocabulary should be a foundational literacy (router, reboot, image, wifi, OS, RAM, CPU, IP, cloud, binary, HTTPS, etc.) part of reading, social studies, math, science, etc.

Cloud computing, web development, mobile apps are introduced in middle school

High School

Classes targeted to specific hardware or certifications (CompTIA, CISCO, etc.)

Secure coding can be integrated and can come after an AP level CS class

Include cutting edge technologies like AI + cyber: automated intelligent systems

Source: MCCE

How many students need to be prepared?

- What percent of current MD high school students would be needed to fill all of the open DC / MD area jobs? (if we could fill them all)
- 390,841 MD public high school students in 2017
- 60,000 open cyber jobs in VA, DC and MD
- If 1 out of every 6 current MD public high school students chooses a career in cyber, the open jobs will be filled in 4 years. (but most jobs are not entry level!)

(http://www.marylandpublicschools.org/about/Documents/DCAA/SSP/20172018Student/2018EnrollbyRace.pdf)
(https://www.cyberseek.org/heatmap.html)

Source: MCCE

Challenges to Cybersecurity for K-12

1. SORTING OUT CURRICULUM
2. TWEAKING CURRICULUM FOR TEACHER COMFORT
3. INTEGRATION OF CYBERSECURITYCURRICULUM INTO VARIOUS SCHOOL DISTRICTS
4. TEACHER PROFESSIONAL DEVELOPMENT TO TEACH CONTENT
5. INTEGRATING CURRICULUM INTO SOCIAL STUDIES, LITERACY AND OTHER AREAS

SOURCE: bit.ly/MCCEcyber

Source: MCCE

Win-Win Situation
High school should inspire and lead to a future

We WIN If students leave high school with:

1. A foundational literacy of technology vocabulary and definition of cybersecurity
2. Reasonable computer skills
3. At least one computer science class that emphasizes problem solving and human computer interaction, with project collaboration and teamwork in a digital world.
4. The knowledge that there is a need for people in CS and cybersecurity with a variety of interesting skills, pay-scales, certifications and advancement options
5. The attitude that they are capable of learning new things and that cybersecurity is challenging and interesting work.
6. Counseling support to match their interests with available options.

Source: MCCE

6 Signs You Have A Quality High School Tech (Cybersecurity) Program

1. A teacher who is passionate about teaching technology and consistently puts in outside time to work with students.
2. A hands-on classroom working on activities students can relate to.
3. Encouragement to earn a certification or learn more through tutoring sessions and peer-to-peer coaching.
4. Good communication about expectations for the classes and opportunities in technology
5. A holistic culture of computer learning through extracurricular clubs and technology competitions
6. Formal ways to connect students to workplace and earning opportunities, including internships and job shadowing days.

Source: A Parent's Guide to the T in STEM Education, Charles Eaton

What Can You Do Next?

- Help identify quality curriculum and professional development opportunities across K-12 cybersecurity arena
- Work with districts to develop plans to integrate and/or create cybersecurity courses for ALL students
- Identify and fix gaps between what is being taught and what needs to be taught
- Find a way to scale, sustain, and broaden participation
  - Socioeconomic
  - Disabilities
  - Gender, ethnic and racial diversity
- Build a stronger pathway for future students
- Obtain resources: hardware, software, networks, contests, public/private partnerships.

Source: MCCE

QUESTIONS?

UNIVERSITY OF MARYLAND
GLOBAL CAMPUS

Formerly UMUC

Nothing used after this slide

- Options range from specific to a multi-disciplinary approach.

- Classes targeted to specific hardware or certification (CompTIA, CISCO, etc.)
- Secure coding can be integrated and can come after an AP level CS class
- Ethics, impact, policy and legal issues may be incorporated into social studies.
- Cloud computing, web development, mobile apps are introduced in middle school
- Encryption and code breaking can be spread throughout K-12
- Understanding how computers work and communicate should start in elementary
- Understanding PII, digital hygiene and citizenship should be a foundational literacy for ALL.
- Essential technology vocabulary should be a foundational literacy (router, reboot, image, wifi, OS, RAM, CPU, IP, cloud, binary, HTTPS, etc.) part of reading, social studies, math, science, etc.
- Include cutting edge technologies like AI + cyber: automated intelligent systems

Source: MCCE

We need a general education solution

Number of public high schools in MD = 180
Average number of students in a CTE pathway through year 4 = 15

If every MD public high school had a full cybersecurity CTE pathway (*Cost = $$$*) there would be 2,700 students graduating each year with some expertise.

This can't be solved with CTE alone. We need students to choose these pathways in the community colleges, technical schools, and universities. We already have many good programs in place.

Top certifications needed require multiple years of study and maturity:
CISSP, CompTIA Security+, GIAC, CISM, CISA

What is the real need?

1. Are current university and community college programs undersubscribed or over subscribed?
    a. If we motivate more high school students, will they have anywhere to go to learn more?

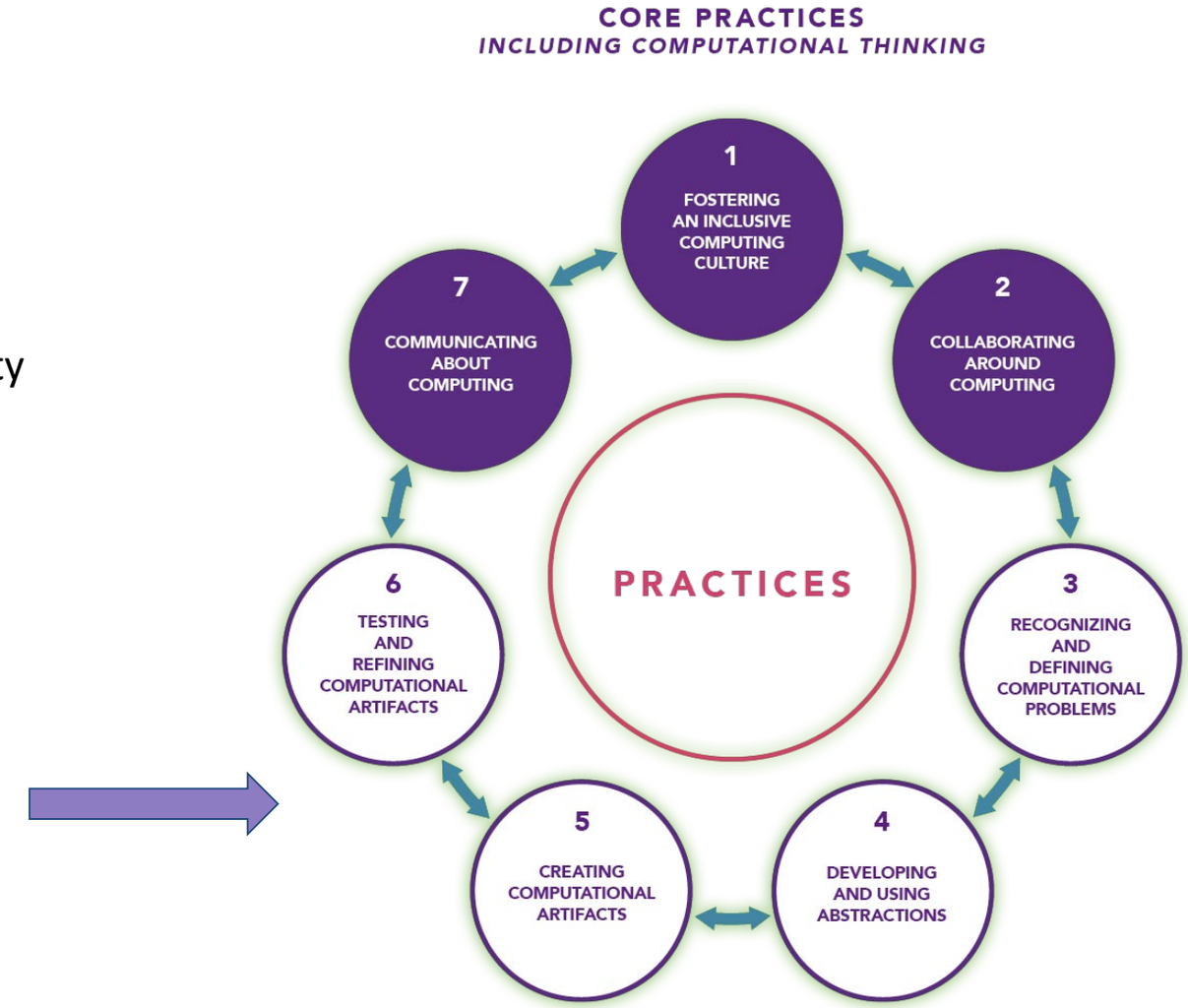
2. The majority of graduating high school students lack the maturity to independently pursue a career.
    a. Studies show that modern teens are emotionally immature compared to previous generations and lack the ability to make logical choices, follow long-term commitments, prioritize, seek wisdom before acting, learn independently, and seek counsel when needed.
    b. So how much experience is needed to reach the maturity levels needed for the cyber workforce where good decision making is critical?
    c. 47.2% of students entering college do not graduate within 6 years and almost 33% change their major within the first 3 years of college. The more background they have for cyber, the more likely they will choose it wisely.

How do we build a pathway to get there?

K-8 : Cover <u>all</u> of the MD CS standards

9-12: Offer core content for ALL students and specialty courses for those with a greater interest.

Incorporate these practices throughout



What's already out there

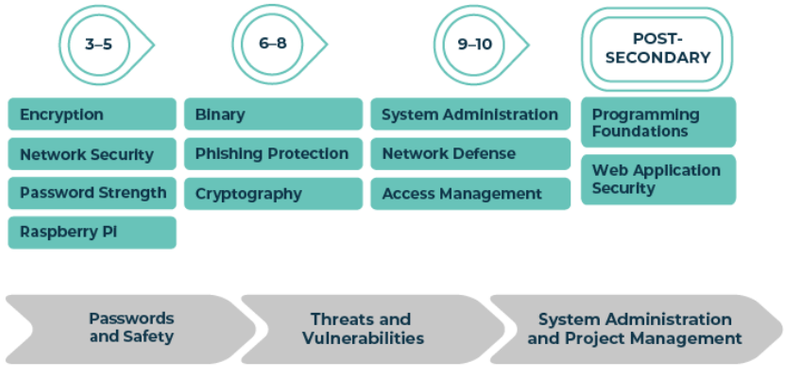
NetAcad free Linux course

Extensive programs in our MD community colleges, trade schools and universities
And outside resources specifically designed for K-12:

GROWING CYBERSECURITY DEVELOPERS A K-12 PROGRESSION

Woz U Education is a model for incorporating computational thinking in the K-12 classroom and accelerating the path to employment for students who choose cybersecurity as a career. Students start with identifying multiple strategies for protecting devices and information from unauthorized access in 3rd grade and transition into writing and creating their own encryption codes. Students may choose elective courses in their Junior and Senior year through concurrent enrollment with a nationally acclaimed coding school and complete the requirement for their certificate shortly after graduation.

WOZ U EDUCATION



Cyber Security by Derek Babb, NE

A curriculum for a high school cyber security course.
https://github.com/DerekBabb/CyberSecurity

This curriculum is designed for a high school computer science course focused on cyber security. Each of the units have activities that could be used with or without prior coding knowledge so the course is customizable to the needs of the given students/teacher.

Topics

- Ethics and Society
- Security Principles
- Classic Cryptography
- Modern Cryptography
- Malicious Software
- Physical Security
- Web Security

Districts are asking for help!

Districts that already have an established computer science program are looking for quality content and PD for courses that cover:

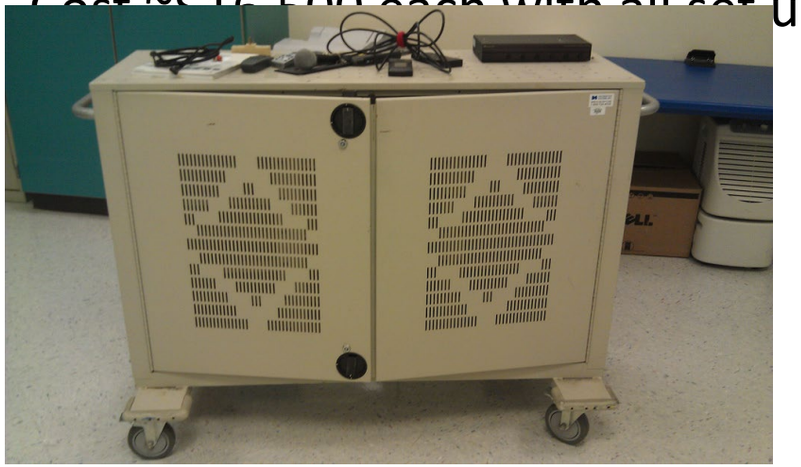
- Linux/Unix and operating systems in general
- Electronics, circuits, Arduino, and IoT
- Robotics with teamwork and problem solving
- App development, website development, web services
- Networks and network security
- Secure coding

What about equity?

What about Baltimore City? Schools don't have computers or reliable internet to offer basic computer classes.

Solution #1:

Laptop carts with access point
Cost ~$16,500 each with all set up



Solution #2:

Raspberry Pi computers with access point
Cost ~$4,000 each with all set up, training
and
mo
ds,

https://www.raspberrypi.org/learning/teachers-guide/physical-setup/

Discussions:

1. Summer professional development 2019. What priorities would you choose?
2. Developing a 6-12 pathway for foundational cybersecurity learning for all students. What do we focus on? Encryption, secure coding, networking, hacking and protecting, digital citizenship, secure web design, AI in cyber, etc. (See MD standards)
   Who should be part of that process?
3. CS Summit, April 2nd at Bowie State. What would be the most useful sessions to offer around cybersecurity assuming that there will be attendees from every district in the state?
4. Resources needed: hands-on operating systems, hardware, networking experiences for a broader range of students. How can we broaden participation with hands-on resources?
5. Contests: what will enable more schools and students to participate?
6. Brainstorm possibilities for possible public/private partnerships

Wrap Up, determine follow up if needed.

Please note: The MCCE can provide teacher PD, support, experiences and district grants. It cannot fund equipment, infrastructure or student-facing materials.