CYBERSECURITY EDUCATION SURVEY FOR MARYLAND PUBLIC HIGH SCHOOLS

September 2021

Contents

Executive Summary

In collaboration with the Maryland State Department of Education (MSDE), the Maryland Center for Computing Education (MCCE), the University of Maryland Global Campus (UMGC), and the National Security Agency (NSA), the National Cryptologic Foundation (NCF) conducted a survey to solicit inputs from all Maryland county and city school districts to advance Maryland cybersecurity education. During the Spring Semester 2021, an online/automated survey was created and made available to the 24 Maryland District Administrators for subsequent dissemination to the teachers, administrators, and counselors within each of their school systems. This report documents the responses of the NCF Cybersecurity Education Survey for Maryland Public High Schools, performs some analysis of these responses, and provides some recommendations for a path forward.

The National Cryptologic Foundation appreciates the help of those who made this study possible with particular thanks to Dr. Rita Doerr who spearheaded and guided the effort along with Dr. Gregory Von Lehmen and Dr. Loyce Pailen from our strategic partner at the University of Maryland Global Campus (UMGC).

Introduction

Cybersecurity is a growing industry worldwide. With over 500,000 job openings in cybersecurity throughout the United States[1], cybersecurity education is a critical national imperative, especially at the secondary level.

Background

The NCF is a non-profit organization created to support the mission of the NSA's National Cryptologic Museum (NCM), the first public museum in the U.S. Intelligence Community. Since 1996, the Foundation has supported the NCM in educating the public on the importance of cryptology in defense of our Nation. One of the NCF's three goals is education. As a nationally reputed provider of assured quality cyber education resources, the efforts of the NCF help to reduce cyber workforce deficits and current skills shortfalls, thereby promoting cyber professions as a fulfilling career choice.

The intended audience for this survey were three groups of educators: (1) teachers, with a varying degree of cyber knowledge – know "a lot" to know "nothing", (2) counselors, and (3) administrators. These educators came from 24 county and city school districts throughout the State of Maryland.

Through this survey, the Foundation hoped to gauge how well the career field of cybersecurity is understood and what the challenges are in developing high school courses and

[1] https://www.cyberseek.org

programs to better prepare students for cybersecurity degrees and careers. To guide the overall survey process, three overarching questions were put forth by the Chair of the NCF Board of Directors:

- What does Cybersecurity Education mean to you?
- What are you doing now in Cybersecurity Education?
- What resources do you need?

Because of the academic and career-related aspects of this survey, a team approach was adopted by the NCF, and members of the following organizations were identified in January and February, 2021 (hereafter referred to as the NCF team):

- Maryland Center for Computing Education
- Maryland State Department of Education, the Division of Career and College Readiness
- National Security Agency, the Office of Academic Engagement
- University Maryland Global Campus, Center for Security Studies, and Office of the President, Cybersecurity

Phased Approach

Once the NCF team was assembled, a phased approach – **Quality Control, Refinement, Development & Distribution, Analysis & Validation** -- was adopted to create, verify, and distribute this survey. Based on the three overarching questions as outlined above, an initial set of survey questions was developed by the NCF team for the teachers, counselors, and administrators. Wanting this survey to be distributed to **all** these groups, regardless of their cyber background, a Likert-style discriminator question was initially asked of each:

"How much do you know about Cybersecurity?"
- A Lot
- Some
- A Little
- Nothing

If a teacher were to select "A Lot" or "Some", they were directed to a different set of questions than if they had responded "A Little" or "Nothing". This "re-direction" method was only used for the teachers; the counselor and administrator responses to that question were just tabulated (reference **General Results**).

Once an initial set of questions was developed for each group, the NCF team wanted to vet these questions with current Maryland educators. During this **Quality Control Phase**, four selection criteria were identified as from which Maryland schools these educators should originate:

- Maryland's five geographic regions (Western, Capital, Central, Southern, Eastern Shore)
- school size (small, medium, large)
- CS/IT program: yes | no
- rural and/or underrepresented

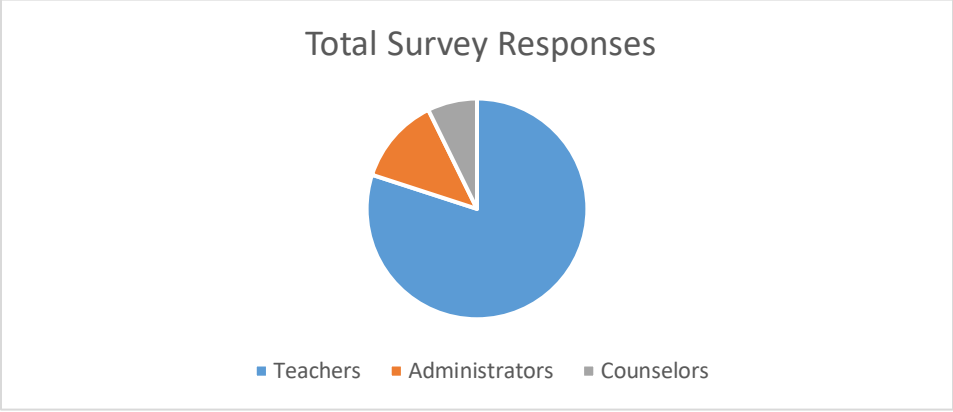
Given these criteria, members of the MCCE and the MSDE identified 12 Maryland educators in mid-February 2021. The **Refinement Phase** began when the NCF team provided these educators with the initial set of survey questions, for all three groups, and asked for their feedback. In early March, the NCF team virtually met with three of these Maryland educators (K, J, T) who provided their invaluable suggestions for survey improvement.

The NCF team then spent the next two months further refining these questions, and then developing and debugging an automated survey, using Microsoft Forms, in which to make these questions available online. As part of this **Development & Distribution Phase**, the NCF team discussed to whom and how best to disseminate this online survey. Knowing that each of the 24 Maryland School Districts had a sole administrator, the MCCE suggested emailing the survey link to the 24 Administrators, and they, in turn, could re-distribute that email to all teachers, counselors, and administrators within their respective school districts. On May 4, 2021, the NCF Education Director emailed the MS Forms survey link, along with a cover letter explaining this effort, to all 24 Maryland School District Administrators.

Within days, responses from the online survey were being tabulated and accumulated. The survey questions were intentionally designed such that responses could not be traced back to any specific school district, school, or individual. The only demographic information that was obtained was a question regarding the overall school population, i.e., under 1000 students, over 2000 students, or in-between. Given the responses, focus groups were not needed to resolve any data ambiguities, thus the **Analysis & Validation Phase** was not conducted. The survey was "live" until June 23, 2021. The next section discusses the overall results of this NCF survey.

Overall Results

As of **June 23, 2021, there were 110 total responses**: 88 Teachers, 14 Administrators, 8 Counselors.



In what follows, excerpts from some of these responses were used to provide data analytical answers to the original three overarching questions.

1) What does Cybersecurity Education mean to you?

Teachers who knew "a lot"/"some" about cybersecurity felt that Computer Science (15 of 28 responses, 54%) is the academic area most relevant to Cybersecurity Education.

Cryptography and Data Communication/Networking were the next most frequent responses with 11 of 28 responses (39%) each.

2) What are you doing now in Cybersecurity Education?

75% (6 of 8 responses) of the **Counselors** indicated that they occasionally bring up cybersecurity as a career option in their conversations with students.

When asked to identify the activities and partnerships related to cybersecurity education that they are involved with, the majority of the **Teacher** responses (from a total of 28) included:

- Teaching or Taking Cybersecurity Courses (19 responses)
- Professional Development (18 responses)
- Cyber Clubs, robotics clubs, etc. (14 responses)
- Not doing anything, but curious to learn more (14 responses)
- Piloting TeachCyber.org Curriculum (one response)

3) What resources do you need?

Administrators indicated that both "Funding $$$" and "Professional Development" (8 responses each) and "Cyber Training/Certifications for teachers and IT admin and STEM Cybersecurity Curriculum" (7 responses each) were needed resources for their schools. An additional suggestion for a needed resource was "More Staff who's dedicated purpose it is to focus on STEM and Tech alone."

Counselors indicated that some of the resources that they need to better advise their students for participating in cyber competitions, extracurricular activities, attending college/universities that offer cybersecurity majors, etc, are:

- "Internships, cyber job fairs, websites"
- "Online bulletin boards, pamphlets"
- "Electives, after school or club opportunities and/or curriculum activities that would be sprinkled into the curriculum in grades 5-10"
- "Local job opportunities as it pertains to career"

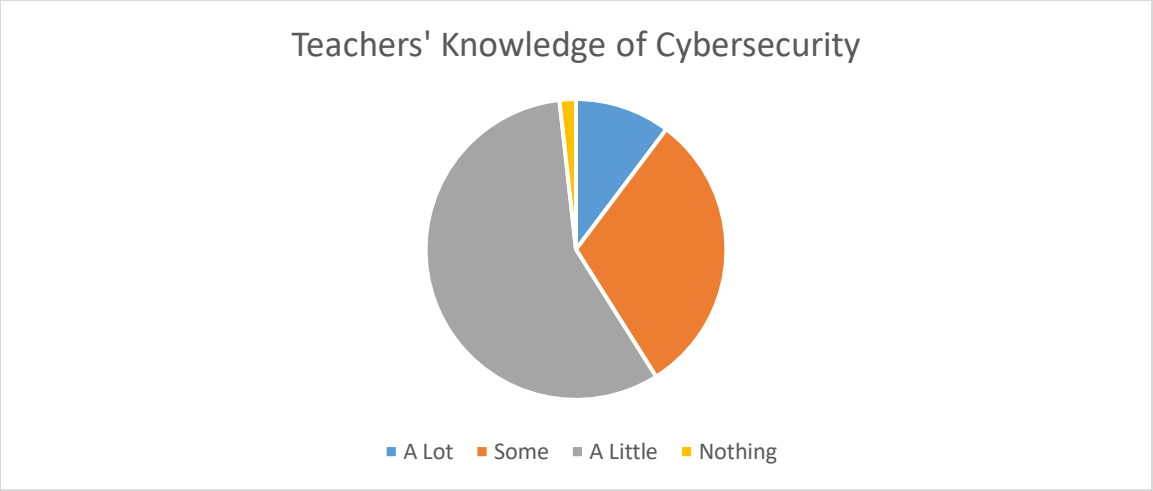
When asked what resources they need to teach cybersecurity that they do not currently have, **Teachers** (28 responses) indicated "Funding $$$" (15 responses) and "Professional Development" (16 responses). The **Teachers** also provided the additional resources:

- "I would like a sandbox so that the students can use WireShark in school so I can help them use it instead of using it at home on their own. It's hard to answer their questions and make sure they are looking at the correct information in the packets."
- "I'm not sure what we should be doing at the elementary level, but I do think we should start teaching the basics before students enter middle school."

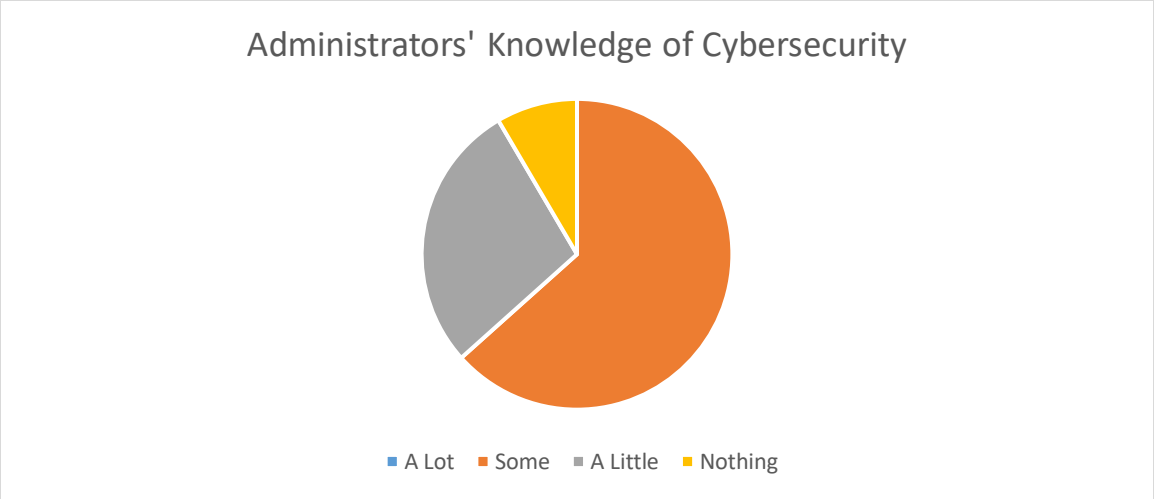
- "This year I piloted the TeachCyber.org curriculum. It is an excellent curriculum. Since I was a pilot teacher a [I] was given free access to the US Cyber Range at Virginia Tech. Using this resource really made the curriculum exciting for students."
- "VMWare is not allowed to be installed on our classroom computers. This is one example of the difficulty we have teaching cybersecurity. I have raspberry pi's to run Linux, but not complete Linux curriculum. Pretty much, teachers are on their own, doing what they can to teach cybersecurity. We need a big overarching plan and support from the district level."

General Results

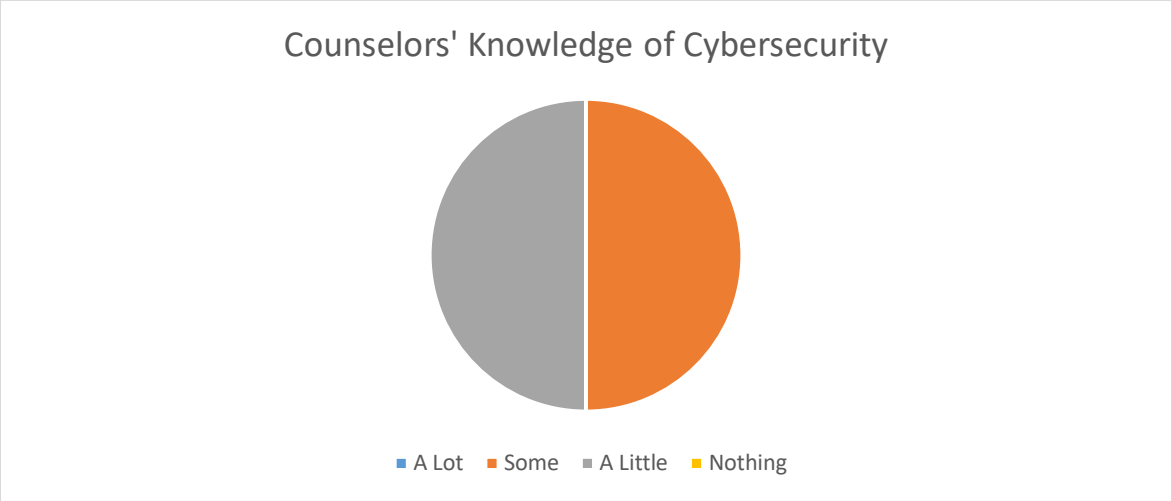
Of the 88 Teachers, seven said that they knew "a lot", 21 said "some", 39 said "a little" and 21 said "nothing" about knowing Cybersecurity.



Of the 14 Administrators, zero knew "a lot", nine knew "some", four knew "a little" and one knew "nothing" about Cybersecurity.



Of the eight Counselors, four knew “some”, four knew “a little” about Cybersecurity.



What else did we learn?

From the **Counselors**, 75% of them (6 of 8 responses) indicated that they see either “a little” or “some” interest in their students in pursuing a career in cybersecurity. When asked about why their students are not interested in cyber careers, they responded: “They may not have much knowledge in it” and “They need more exposure other than counselor’s office.”

From the **Teachers**, when asked what perceptions are barriers to teaching and learning cybersecurity, the leading responses were “lack of understanding about the importance of cybersecurity” (17 responses), “Cybersecurity is too technical” and “Lack of understanding of the cybersecurity field” (16 responses each). The Teachers further noted that there is a lack of exposure to cybersecurity due to 1) No Computer Science classes offered at the school; and 2) No access to computers, laptops, or tablets.

From the **Administrators**, an additional suggestion for a needed resource was "More Staff who's dedicated purpose it is to focus on STEM and Tech alone."

What result was the most surprising?

The need for awareness building – what cyber is and the breadth of jobs – was the most interesting response from the **counselors**, **administrators**, and the 39 of the "know a little" and 21 "know nothing" **teachers**.

Which result was the most resounding?

The most resounding (and consistent) response from all three groups was the need for additional funding and Professional Development and Cyber Training/Certifications for teachers and IT admin and STEM Cybersecurity Curriculum (7 and 8 responses, respectively) were needed resources for their schools in cybersecurity instruction.

Recommendations

Based on the NCF Education Program Initiatives and the responses from this survey, the following are some recommendations for short-term actions:

- Continue with the development and dissemination of the High School **Cybersecurity Curriculum through Teach Cyber** -- especially in Maryland as many survey comments centered around the lack of one central set of standardized curricula for cybersecurity at the high school level to include access to Cyber Ranges for laboratory exercises ["we need a big overarching plan and support from the district level"]
- Increase the level of **Online Virtual Learning through NEPRIS** as there was a specific survey comment about having guest speakers from NCF/NSA
- Continue with the development and disseminator of the **CLARK Curriculum K-12 Repository**
- Disseminate **NCF's Cybersecurity Booklet for Middle School** as many of the survey responses stated that they wanted their incoming high school freshmen to know about cyber threats/hacking/ability to think like an adversary

Based on the NCF Education Program Initiatives and the responses from this survey, the following are some recommendations for new, long-term initiatives:

- Develop and promulgate Teacher Professional Development in cybersecurity based on **NCF's Cybersecurity Curriculum Guidelines and TeachCyber HS materials**.
- Develop **ANOTHER middle school booklet** containing suggested topics that the survey respondents provided (hex, binary, decimal conversion to ASCII, encryption methods, etc.)

Distribution of Final Report

- **National Cryptologic Foundation**: Dick Schaeffer, Laura Nelson, Mark Loepker
- **Maryland State Department of Education**: Marquita Friday, Elissa Hozore
- **Maryland Center for Computing Education:** Dianne O'Grady-Cunniff, Megean Garvin
- **University of Maryland Global Campus**: Loyce Pailen, Greg Von Lehman
- **National Security Agency:** A2 (Diane Janosek), A29 (Lynne Clarke, Ashley Greeley), C5 (Rita Doerr, Natalie Janiszewski), E&P (Natalie Laing), P3 (Brenda Martineau), P33 (Pamela Jock, Lori Robey)
- **Maryland Congressional Officials**: Congressman Dutch Ruppersberger
- **National Cybersecurity Director**: The Honorable Chris Inglis
- **Maryland Educators**: Kimberly Mentzell, Justin Serota, Tommy Thompson
- **Maryland Cybersecurity Council, Subcommittee on Workforce Development:** State Senator Katie Fry Hester (chair)
- **Ft Meade Alliance:** Steve Tiller

APPENDIX

Specific Results (statistics and direct quotes from survey responses)

➔ Counselor

- Of the **8 counselors**, 4 knew some and 4 knew a little about Cybersecurity
- Collectively, they provide counseling to grades ranging from 8th to 12th.
- 75% (6 of 8) responses indicated that they occasionally bring up cybersecurity as a career option in their conversations with students.
- When asked what resources they need to better advise their students for participating in cyber competitions, extracurricular activities, attending college/universities that offer cybersecurity majors, etc., they responded (in part):
  - "Internships, cyber job fairs, websites"
  - "Online bulletin boards, pamphlets"
  - "Electives, after school or club opportunities and/or curriculum activities that would be sprinkled into the curriculum in grades 5-10"
  - "Local job opportunities as it pertains to career"
- When asked what resources they use or point students to for career-related information, the overwhelming response was "Naviance" (7 of 8 responses)
- 75% (6 of 8) responses indicated that they see either "a little" or "some" interest in their students in pursuing a career in cybersecurity
- When asked about why their students are not interested in cyber careers, they responded:
  - "They may not have much knowledge in it"
  - "They need more exposure other than counselor's office."

➔ Administrator

- Of the **14 administrators**, 9 knew some, 4 knew a little, and 1 knew nothing about Cybersecurity
- Regarding which grades that their schools teach, the responses included:
  - 9-12 (6 responses)
  - 6-12 (4 responses)
  - K-12 (1 response)
  - District Admin, Building Level Administrator, N/A (3 responses)
- The **administrators** indicated that both Funding $$$ and Professional Development (8 and 9 responses, respectively) and Cyber Training/Certifications for teachers and IT admin and STEM Cybersecurity Curriculum (7 and 8 responses, respectively) were needed resources for their schools for cybersecurity instruction. An additional suggestion for a needed resource was "More Staff who's dedicated purpose it is to focus on STEM and Tech alone."

➔ Teacher

- Of the **88 teachers**, 7 knew a lot, 21 knew some, 39 knew a little, and 21 knew nothing about Cybersecurity

- Teachers with "a lot" or "some" cybersecurity knowledge (**28 responses**)

    - When asked about what resources do you need to better advise your students for participating in cyber competitions, extracurricular activities, attending college/universities that offer cybersecurity majors, they responded (all direct quotes):
        - a course for Cybersecurity / a curriculum
        - any information we can receive including what resources are approved for use
        - Books, Access to virtual labs and scholarship funds.
        - Colleges with cybersecurity degrees
        - Consolidating information regarding cyber competitions based on local area.
        - Current programs, regional/national program options, pre-requisites as well as predatory curriculum suggestions to better prepare our HS students for the rigors of College level Cyber Security academics
        - Cybersecurity certifications vs college?
        - extracurricular activities, real world connections to how cyber impacts your life.
        - For participating in Cyber competitions, mentoring.
        - For professional development, it would be nice to be able to get a certificate, like a Security+. I would just need more training, knowledge, and be able to attend conferences (either virtual or in-person) to better my understanding. Like it would be nice for conference to have scholarships for teachers (i.e. Schmoocon's Fund A Student) that could attend. For other resources, it is technology and support from central office. Also, cost effective virtual machines.
        - funding
        - Guest speakers from NCF/NSA; Mentors for Cybersecurity seniors; Activities and labs
        - I do not need additional resources
        - I guess everything
        - I have been doing some of this throughout this year. The biggest limitation for me is time.
        - I have no clue.
        - links, and email offerings prior to when the events occur
        - Materials of instruction, booklet, brochures, college/university information.
        - Money for FBLA and other competitive events. CyberPatriot has changed in recent years and is too driven by a few programs that out resource 99% of teams.

    - More cyber PD for "best practices". I want my students to get the core concepts of cybersecurity, so I want to be aware of best instructional strategies.
    - N/A; None - this is outside of my content curriculum; not sure
    - Opportunities for them [students] (some type of calendar or list)
    - PD from professionals who offer the competitions on how to solve some of the more complicated problems and in state info on colleges who offer this track.
    - resources and hands-on activities; Teaching material and hardware
- When asked what resources you need to teach cybersecurity that you do not have, the two majority responses were "Funding $$$" (15 responses) and "Professional Development" (16 responses). Other resources provided were (all direct quotes):
    - I would like a sandbox so that the students can use WireShark in school so I can help them use it instead of using it at home on their own. It's hard to answer their questions and make sure they are looking at the correct information in the packets.
    - I'm not sure what we should be doing at the elementary level, but I do think we should start teaching the basics before students enter middle school.
    - This year I piloted the TeachCyber.org curriculum. It is an excellent curriculum. Since I was a pilot teacher a [I] was given free access to the US Cyber Range at Virginia Tech. Using this resource really made the curriculum exciting for students.
    - VMWare is not allowed to be installed on our classroom computers. This is one example of the difficulty we have teaching cybersecurity. I have raspberry pi's to run Linux, but not complete Linux curriculum. Pretty much, teachers are on their own, doing what they can to teach cybersecurity. We need a big overarching plan and support from the district level.
- When asked what the top three things (foundational knowledge, technical or otherwise) that you want your students to know before coming to high school, they responded (select direct quotes):
    - 1. What specifically is cyber security? 2. How do we protect our personal identifiable information? 3. How do we minimize risk?
    - awareness of possible threats to their internet experience, basic knowledge of potential cyber problems, how to recognize hacking
    - 1. Basic computer literacy (hardware & software) 2. How to work in a team setting 3. Financial literacy & everyday math
    - Before taking cybersecurity, students should take Computer Science Principles to get foundational knowledge in data, the internet, programming, global impact of computing, and cybersecurity.
    - Binary, Hex, Decimal conversion to ASCII, Encryption Methods, Data Compression
    - 1. Computational thinking abilities 2. Logical reasoning 3. Ability to think like an adversary
    - Computer ethics, respect for the "keys to the kingdom" and patience

- 1. Cyber threats are real 2. Everyone on the web is not your friend. 3. What you don't know can hurt you.
- foundational knowledge, technical understanding, how to keep their personal information secure
- I would like that they have computational thinking or problem-solving skills. It would be nice for them to know basic programming and digital literacy concepts. It would also be good for them to know basic information about cybersecurity.
- social media is forever
- 1. That once it is out there in the web, it is there forever 2. Be cautious 3. THINK
- Why cybersecurity is necessary to understand.

- When asked what perceptions are barriers to teaching and learning cybersecurity, the leading responses were "lack of understanding about importance of cybersecurity" (17 responses), "Cybersecurity is too technical" and "Lack of understanding of the cybersecurity field" (16 responses each)
- "Other" perceptions include (all direct quotes):
  - Cyber security changes so often, impossible to keep up with
  - **Cybersecurity and computer science are just for people who like to play video games. (NB: Rita's fav)**
  - The goals of Cybersecurity education need to be established by the school system authorities before judgements can be made about barriers.
  - Lack of exposure to cybersecurity due to 1) No CS classes offered at the school; 2) No access to computers, laptops, or tablets.
- When asked what would be useful to you if you wanted to learn more about cybersecurity, the overwhelming response (18 responses) was "Professional Development"
- "Other" resources for learning more about cybersecurity include (all direct quotes):
  - Curriculum needs to be adopted before learning needs can be identified.
  - Contacts with cybersecurity professionals so they can assure that I am heading the students in the right direction.
  - Current or frequent web update/trends resources
  - Online resources. Cybersecurity is changing so rapidly, the most up to date info is found on the internet.
- When asked what are the resources available to you for professional development, the overwhelming response was "Maryland Center for Computing Education (MCCE)" (17 responses)
- "Other" resources available for professional development include (all direct quotes):
  - Classes for Cybersecurity
  - I am one of the TeachCyber Pilots.
  - I don't know what other resources are available. (4 responses)
  - Partnership with Post-Secondary Institution and access to their curriculum.
  - TeachCyber

- We spend most of our PD time during the year doing district specific PD which doesn't leave time for PD of our choice.

- From the 28 teacher "a lot"/"some" responses, here is the percentage of them that feel each of the following skill or academic area is **VERY IMPORTANT** to cybersecurity education:
  - **Computer Science: 54% (15/28)**
  - Engineering: 14% (4/28)
  - Cryptography: 39% (11/28)
  - Math: 18% (5/28)
  - Data Comm/Networking: 39% (11/28)
  - Web Design and Development: 11% (3/28)
  - IT and Systems Administration: 29% (8/28)
  - Civics: 18% (5/28)
  - Social Science: 11% (3/28)
  - Language: 14% (4/28)
  - Software Development and Programming: 32% (9/28)
- When asked what are other important skills or academic areas in Cybersecurity Education (in addition to the above), the following were provided (all direct quotes):
  - A curriculum needs to be chosen before this question can be meaningfully answered.
  - Cable making – fiber and copper
  - Determining the end user of your website/data/program
  - Ethics
  - extremely important – to tie in the what and why
  - none (2 responses)
- When asked to identify the activities and partnerships related to cybersecurity education that they are involved with, their majority responses included:
  - Teaching or taking Cybersecurity Courses (19 responses)
  - Professional Development (18 responses)
  - Cyber Clubs, robotics clubs, etc. (14 responses)
  - Not doing anything, but curious to learn more (14 responses)
- For the preceding question, the one response for "Other" cybersecurity curriculum development activities was "Piloting TeachCyber.org curriculum"
- When asked about which cybersecurity educational resources they are familiar or have used, the majority responses (based on 28 respondents) were:
  - None (21 responses)
  - TeachCyber.com (12 responses)
  - Codehs.com (11)
  - NICE K-12 Cyber Curriculum Repository (10 responses)
  - Cyber Range (10 responses)
- For the preceding question, "Other" familiar cyber resources included:
  - cyber.org
  - CISCO packet router
  - CyberStart
  - I was not aware of the above

        - I have also used some resources from the DefCon Hacking Conference (as well as other conferences). I have used picoCTF as extra practice.
    - When asked about how often they involve parents in cybersecurity awareness training and topics that they teach and/or advise their students, the breakdown is as follows:
        - Sometimes – 13/28 responses, 46%
        - Never – 9/28 responses, 32%
        - Often – 5/28 responses, 18%
        - Always – 1/28 responses, 4%

- Teachers with "a little" or "nothing" cybersecurity knowledge (**60 responses**)

    - The **39 teachers** with "a little" knowledge, teach the following courses:
        - Algebra/Math/Pre-Calc, various regular/AP Computer Science, various regular/AP History, various Biology/Zoology, Band and Theater, Chemistry, Criminal Justice and Corrections, Business/Econ/Finance, Engineering, Fine Arts, English
        - History, Hospitality & Tourism Management, Special Education (Geometry & English & Life Skills), Instrumental Music, Interactive Media, Library, Masonry & Construction Design & Management, GIS/Engineering
        - Music/Theatre, PE 10 & 12 & Athletic Skills, various PLTW Science/Computer Science/Cybersecurity/Engineering, Spanish, Tech Education, World Language
    - The **21 teachers** with "nothing" knowledge, teach the following courses:
        - AP US History, Algebra 1 & 2/High School Math, Chemistry, Communication Arts/Yearbook, Computer Science Essentials, English, Environmental/Physical Science, ESOL, Foundations of Tech/Computer Science, Government & US History, Music, Physical Education, Special Education, Social Studies, Visual Art, World Languages
    - Of the 60 responses, **26 teachers** indicated that they would be interested to learn more about Cybersecurity, while 16 said No and 18 said Maybe

- When asked if they wanted to learn more about cybersecurity, what would be useful to them … they overwhelmingly responded (23 of 60 responses) with "Professional Development in Cybersecurity" … "Other" responses (2) indicated that "All of the Above" and "Creativity … outside the box thinking, promotion and cybersecurity" were also useful
- When asked what are the current resources available to you for professional development, the **43 responses** varied with the majority of them (**24 responses**) "unsure/didn't know/have no idea/none that I know of": "code.org, county generated, county PD's and opportunities through codeintheschools.org and marylandcodes.org, desktop and laptop and iPad, Google Meetings and other colleagues in my county, Guest speaker and Break Out Groups, I run PD that is mostly centered around teaching

strategies and integrating technology, I will be taking training for PLTW Cybersecurity in June 2021, Internet/Board of Ed/local community, Just what PLTW provides, online learning/in-person classes, past professional development and current explore computer science curriculum, PD days/built into calendar and Zoom meetings, PLTW training and College Courses paid out of pocket, School-based, Supervisor made college courses, We have several opportunities throughout the school year"

➔ **Final Section**

- When asked about into which other high school subjects cybersecurity education could be incorporated, the majority responses of the 110 respondents included:
    - Math (77 responses)
    - Science (76 responses)
    - Social Studies (70 responses)
- Regarding the previous question, the following are their 61 responses as to how cyber education could be incorporated (all direct quotes):
    - All students need to know how to protect their data
    - Any topic that concerns real life can be inserted into curriculum; HOWEVER, even one class period is taking away from the core of a curriculum. Teachers, especially EVERY English teacher gives up a few hours a year to "necessary" extras because, as a group, the English teachers see each student in the school every year.
    - As part of reading material
    - By getting an expert to teach it
    - Co -teaching, competitions, performance - based projects, ISTE standards
    - Coding, laws
    - Computer Science
    - Create a program like criminal justice at the tech centers
    - Cross-curricular activities can be cultivated in those subject areas.
    - Cyber education can be incorporated into all facets of life. It is very because all disciplines cross over or connect to one another.
    - Cyberbullying in health; Online language etiquette in English; Electricity in science; The interplay between cyber security and international relations, or the how the internet of things is impacting society in social studies, cryptography in math.
    - Cybersecurity is important and should be included within a technology course for all students. However, I disagree with attempting to incorporate it (beyond organic discussions surrounding projects, etc) as a requirement in other content areas. This would lead to inconsistent communication of this information, as well as frustration within other content areas. Students should have a basic knowledge of cybersecurity before entering high school and develop that knowledge as needed during high school within their technology courses.
    - Cybersecurity lessons encompass more than STEM concepts. Lesson activities can and should include how cybersecurity impacts our daily lives (e.g., important for protecting our medical data (health), how to communicate cyber concepts over

multiple languages, and recognizing digital patterns in binary & coding can be seen as an art form).
- Cryptography (encryption) could fit into math.
- discussions included in the lessons
- Ethics - Misuse of information and how it is handled by the law enforcement community. Intellectual property - projects that are created in science, English and music/art.
- Every 21st century student using technology in the classroom needs to be informed about cyber security.
- Examining the role of the cyber world in all aspects of modern culture and politics as well as how it would function at a technological level
- For example, being multi-lingual would be helpful.
- History of and current events related to cyber security fit well in Social Studies.
- History of Cybersecurity in Social Studies, Cryptography, and data in Mathematics.
- I am a Technology Education Teacher. I believe it can be incorporated in CTE courses.
- I don't know/unsure/idk (NN responses)
- I don't know that it can be incorporated in those subjects.
- I don't think that specific network defense concepts can be taught in these classes, but there are cross curricular connections (more theory) that can be made.
- I just feel it fits into that curriculum.
- I mean pretty much all subjects can talk about cybersecurity in one way or another. However, this shouldn't be the means for which cybersecurity or computer science is taught.
- I think it could be incorporated in a Technology class such as Foundations of Technology or in the Advance Technology classes.
- I think it could, but with the current situation, most of the subjects are focusing on the power standards and will not be looking to infuse something new.
- In math, how coding works. In social studies, how laws and rights are incorporated.
- Incorporating a topic is a way to avoid the more important question. What topics should not be taught in the domain?
- It can be used to supplement curriculum on coding and computer science.
- It could be a unit of study done at the beginning of each course
- It could be incorporated in technology education courses and/or computer classes. There are too many testing demands on teachers to incorporate one more thing into their curriculums. While this may be an important topic to teach, I don't believe it is helpful to force it upon teachers who are already overwhelmed.
- It should be a thread that runs through all classes. Not all content areas are going to dedicate a week or a quarter to the topic but when it is relative to a topic it should be integrated.
- It touches all aspects of our lives. It is everywhere and impacts everything.
- It would be great for computer science
- Math - binary and underlying mathematical foundation to computer science/cyber

    - Math - Modular Arithmetic and primes for public key encryption; Social Studies - vulnerabilities with hacking government agencies
    - Math and science can investigate how computers and the internet function and can be manipulated. Social Studies can look at current events when cyberattacks happen and discuss how and why they happened.
    - Not sure but blended lessons are often helpful
    - Poster/public awareness artwork, instructional illustration art
    - Problem based learning in the respected content area
    - readings, current events (cyber bulling, cyberattacks, ransomwares, etc) crunching numbers and encryption / cyphers, guest speakers, opportunities for internships
    - Research
    - Safe Usage
    - Science/Social Studies - how cyber-attacks work/effect various groups of people; Math - cryptography, how it works at the algorithm level.
    - Since most classes are technology based, it would make sense for students and especially teachers would be aware of this topic.
    - Social Studies could help explain cybersecurity by going over major events where cybersecurity was a key factor. Math and Science could delve more into the programming if they have the time and resources.
    - Statistics; Trends; Civics/morals
    - Teaching algorithms
    - Through existing technology courses like computer science and foundations of technology. Bring back shop class and combine with one of those as a yearlong course.
    - Using computer science and learning to coding skills which require math and science
- Of the **110 total responses**, 59 were from "Under 1000 Students", 45 were from "1001-2000 Students", and 6 were from "Over 2001 Students" regarding school population