Incorporating Cyber Competencies in K-12

Rachel M. Stange
Bethany College
Bethany, WV, USA
Email: rstange@bethanywv.edu

***Abstract*—Over the past several years, the kindergarten through twelfth (K-12) community has been told to include computer science and cybersecurity in all curriculum. However, the K-12 community does not have the proper knowledge to do so. This paper includes a guide on what to teach to meet the requirements, how to teach it in order to engage students, and how to incorporate it into the curriculum. This guide is different from others because it works with new or existing curriculum and it incorporates the entire K-12 community.**

Keywords- Computer Science; Cybersecurity; K-12 Education; K-12 Curriculum.

I. INTRODUCTION

The author's efforts started out to help her peers and have since spiraled into a crusade to improve cyber competencies within K-12. Two other students who were bullied through cyber stalking and classroom discussion boards had an impact on me. During my sixth grade year, a fellow student killed herself after being cyberbullied, and school officials were unaware. Amanda was a 14-year-old girl from my local community who was cyber stalked, abducted, raped, and left for dead, but sadly, local educators talking about these topics did not know of her story. Now, the book [1] telling her story is in school libraries and used in English classes. Amanda and her mother speak to ninth grade health classes in hopes to prevent this from happening to others. Amanda's story has been combined with two other stories to create the movie *Finding Faith* [5].

In 2016, President Barack Obama released the Computer Science (CS) For All initiative. The goal of CS for All is to teach K-12 students about computer science and provide them computational thinking skills [2]. The issue with CS for All is that many K-12 educators are not knowledgeable in computer science and cybersecurity. As many K-12 school systems are trying to add computer science and cybersecurity into the curriculum, they are realizing that they tend to teach cyberbullying, cyber safety, and certifications without providing educators the needed education to fully understand the fundamentals of computer science and cybersecurity. This is often due to administrators and educators themselves not understanding what cyber competencies are actually needed due to constantly changing fields. At the same time, K-12 continues to teach the Generation Y (Millennials) way. Studies show that social engineering, hacking and defending, cyber awareness, and personal connections have more impact on Generation Z and Generation Alpha students [14].

To many people's surprise, Generation Z is more similar to older generations than Generation Y which means that most of the educational changes put into place for Generation Y needs to be reversed. Generation Y, or Millennials in the United States, do have a few differences from Generation Z, in part because of the majority of the group's parents being Generation X. Due to lower attention span, Generation Z want 'snackable' content meaning that one communicates in bite-sized messages [14]. To reach Generation Z, content must become visually based with text being left as a witty caption, headline, or replaced by an emoji. A large portion of Generation Z have a digital footprint, but they do not know what it is, how it is affected, or that googling themselves actually puts their information into Google's repository to have their information appear higher in the results [14] Generation Z is truly a 'digital first generation' and has a very high trust level which is why it is important to ensure they are taught by cyber competent educators.

Currently, K-12 students are getting the impression from educators that computer science and cybersecurity is just programming. This is seen in many school systems when looking at the curriculum and standardized testing. For example, there is a new high school in Virginia, USA that is supposed to focus on computer science and cybersecurity education, but when you look at the curriculum, they are just teaching coding and different coding concepts. For those educators who are trying to teach more than programming they are struggling as they are using canned lessons to teach students. Canned lessons are lessons that have been made by qualified educators, educators who know the material, for educators that do not know the material to use. The issue with canned lessons is that the educators do not know the material, so they are teaching how to use the system or program and not the concept behind the system or program.

The traditional way of fighting cyberbullying is giving the definition and examples students cannot relate to. The traditional way of fighting cyberbullying is ineffective with Generation Z and beyond because they have heard the same thing for so long, so they are no longer listening. The best way to address cyberbullying is to educate on the issues that lead to cyberbullying by using cyber competencies.

In Section 2, the four main cyber competencies are described and examples of how to present to students are

 ISBN: 978-1-61208-764-1

given. In Section 3, the additional cyber competencies are described and examples of what to present to students are given. In Section 4, the solution model for including cyber competencies in K-12 is presented. In Section 5, the success of using this model and this model's development is given.

II. MAIN CYBER COMPETENCIES

The four main cyber competencies are digital footprints, social media, security, and cyber laws. The components of the four cyber competencies are shown below in Figure 1.

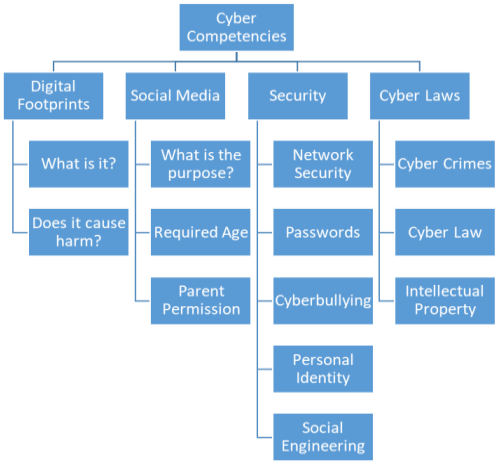

Figure 1. Cyber Competencies & Components [12].

For the digital footprint competency, one must explain what they are, how they help sites and stalkers track one, and how privacy is being given up. Students need to understand all the information online posted by them or by those with access to their social media sites. The goal of the digital footprint competency is to stress to students that people learn about them from their actions on the Internet of Things (IoT). People learning about one online use what one searches, where one searches, what one posts, and what others post about one or in response to one. The easiest way to teach this competency is by using nine phrases, shown below in Figure 2.

1. Don't be a DIGITAL DUMMY: Get real! The Web is **public** and **permanent**
2. Don't be a DIGITAL GOSSIP: Talking about others negatively, makes you look shallow
3. Don't be DIGITAL WEAK SAUCE: Don't let friends influence your better judgement
4. Don't be a DIGITAL DIVA/DIVO: Inappropriate Screen names/pictures & legal issues
5. Don't be a DIGITAL DAREDEVIL: Be careful about sites & friends
6. Don't be a DIGITAL CREEPER: Be careful about what you download, look at, even for a laugh
7. Don't be a DIGITAL MEAN KID: Don't hide behind your computer
8. Don't be a DIGITAL DORK: Information about you is impossible to remove 100%
9. Don't be a DIGITAL PRIVACY KIDDIE: There are always ways to get around privacy settings

Figure 2. Digital Footprint Competency Phrases [14].

When giving examples, educators should be able to connect them to the phrases and make sure they are able to be related to by the students. An example for phrase three is if someone posts something that you view as inappropriate, do not join the conversation unless it is in an attempt to encourage mature and responsible comments. For phrase seven, have students think about what their digital posts will say about them as a person to others. A phrase eight example would be, just like a tattoo on your thigh, an embarrassing post or tweet can last a lifetime.

For the social media competency, explain the purpose of social media sites, why there is required age limits, and the legal consequences of lying about your age to create an account. For example, you are supposed to be sixteen-years-old to use SnapChat, but many educators encourage SnapChat use in their classrooms for students under that age. SnapChat is a mobile application that allows pictures, messages, and short videos to be sent to others with them only being available for a limited amount of time. Generation Z and Alpha students have heard several times that they have to be a certain age and the purpose of social media, so keep this part of the lesson short. The social media competency is mainly taught to students with examples that allow educators to point out good and bad pieces of the situation. Two examples of cyber issues related to social media that can be real life examples used when teaching this competency is Jojo Siwa and the *Blue Whale Challenge*.

JoJo Siwa is a 16-year-old from Nebraska, who became famous after being on *Dance Moms*, *Abby's Ultimate Dance Competition*, and her upbeat songs. During a TV interview she said that she turned the commenting feature on her Instagram off after someone posted a bad comment. However, commenting is still on for Instagram and she never considered changing her settings on YouTube. During another TV interview, she encouraged children ages four to thirteen to follow her on Instagram and YouTube. Talking point one is that Instagram requires you to be 13 years of age to create an account, but even at that age parent approval is still needed. Talking point two is children ages 4-13 should not be creating accounts on YouTube to follow because they should be using YouTube Kids, which has more security protocols as they expect younger members of society to be using it. Talking point three is parent approval should be obtained before creating an account on any social media sites. Talking point four is that famous people and friends should not influence whether you have social media.

The *Blue Whale Challenge* is a challenge that exists on YouTube. The challenge is linked to human trafficking and forced suicide. Teenagers appear to be drawn into online forums where suicide was being discussed. In those forums, blue whale memes where being shared. But the idea of a sinister game, one that slowly roped in vulnerable teens and led them down an increasingly tortured path to suicide, seems th be a simplistic explanation for a complex problem. Participants of the *Blue Whale Challenge* have a whale drawn on their wrist. The last challenge is to either run away into human trafficking or to kill yourself. Talking point one is if you ever find yourself in this situation or know someone in this situation, then you need to tell a trusted adult immediately, even if told or asked not to. Talking point two is that misuse of YouTube needs to be reported.

For security competency, talk about network security, passwords, personal identity, social engineering, and cyberbullying with how they are all interconnected. For example, the social engineering discussion should include geotagging, background of pictures, and the amount of information shared online. The network security discussion

 ISBN: 978-1-61208-764-1

should be about the differences in public and secure wi-fi and when it is safe to connect to public wi-fi.

For the cyber law competency, explain the categories of cybercrime, intellectual property, the categories intellectual property is broken into within cyber laws, and the new cyber laws being put into effect. Intellectual theft is stealing or using without permission of someone else's intellectual property. Intellectual property is protected by patent for inventions and copyrights in creative pursuits such as music, photos, and poems. Cyber law is any law that applies to the Internet and Internet related technologies. The categories of cybercrime, which should be discussed with students are people, property, and government. Cybercrimes against people include cyber harassment and stalking, distrubtion of child pornography, spoofing, credit card fraud, human trafficking, identity theft, and online related libel or slander [14]. A real life example of a cybercrime against people is in 2017 journalist Juan Thompson was sentenced to five years for stalking former girlfriend Francesca Rossi. Cybercrimes against property include Distributed Denial of Service (DDOS) attacks, hacking, virus transmission, cyber squatting, computer vandalism, copyright infringement, and Intellectual Property Rights (IPR) violations [14]. A real life example of cybercrime against property is the Wanna Cry ransomware attack of 2017 which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin currency. Cybercrimes against government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software [14]. An example of a cybercrime against government is the 2016 election intrusion.

III. Additional Cyber Competencies

For the high schools that offer computer science and cybersecurity courses there are two additional cyber competencies that are to be taught to students in those courses. The two additional cyber competencies are computer science and cybersecurity. The components of these two competencies are shown below in Figure 3.

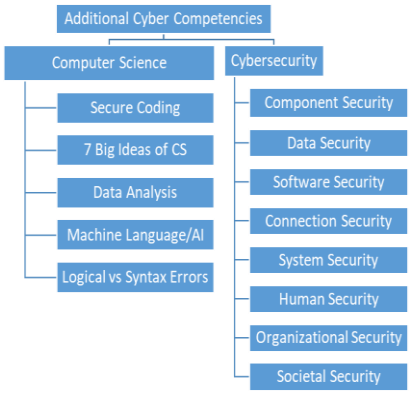

Figure 3. Additional Cyber Competencies & Components.

The computer science competency aligns with CSTransfer2017 [7] so that it allows for better flow from K-12 to college. CSTranfer2017 created by the Association of Computing Machinery (ACM) Committee for Computing Education in Community Colleges (CCECC) is a computer science curriculum guide for Associate Degree transfer programs [7]. For the computer science competency, teach secure coding, the seven big ideas of computer science, data analysis, machine language and Artificial Intelligence (AI), and logical vs syntax errors. The seven big ideas of computer science that should be taught are shown below in Figure 4.

1. Computing is a creative human activity that engenders innovation and promotes exploration
2. Abstraction educes the information and detail to focus on concepts relevant to understanding and solving problems
3. Data and information facilitate the creation of knowledge
4. Algorithms are tools for developing and expressing solutions to computational problems
5. Programming is a creative process that produces computational artifacts
6. Digital devices, systems, and the networks that interconnect them enable and foster computational approaches to solving problems
7. Computing enables innovation in other fields including science, social science, humanities, arts, medicine, engineering, and business

Figure 4. Seven Big Ideas of Computer Science [14].

The cybersecurity competency aligns with Cyber2y2020 [6], CSEC2017 [4], and the Accreditation Board for Engineering and Technology (ABET) so that it allows for a better flow from K-12 to college. Cyber2y2020 created by the ACM CCECC is a cybersecurity curriculum guide for Associate Degree programs [6]. CSEC2017 created by an Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8) joint taskforce is a cybersecurity curriculum guide for post-secondary degree programs [4]. The cybersecurity competency aligns with ABET's program accreditation criteria for Associate Degree programs.

For component security, teach the security aspects of the design, procurement, testing, analysis, and maintenance of components integrated into large systems. For data security, teach the protection of data at rest, during processing, and transmit. For software security, teach the development and use of software that reliably preserves the security properties of the protected information and systems. For connection security, teach the security of the connections between components, both physical and logical. For system security, teach security aspects of systems that use software and are composed of components and connections. For human security, study the human behavior in the context of data protection, privacy, and threat mitigation. For organizational security, teach how to protect organizations from cybersecurity threats and managing risk to support successful accomplishment of the organizations' missions. For social security, teach the aspects of cybersecurity that broadly influence society as a whole.

IV. Solution

The solution to the problem has four steps, as shown below in Figure 5. This solution model has had a positive

 ISBN: 978-1-61208-764-1

impact in reducing the amount of K-12 cyber distress for the many school districts using it.

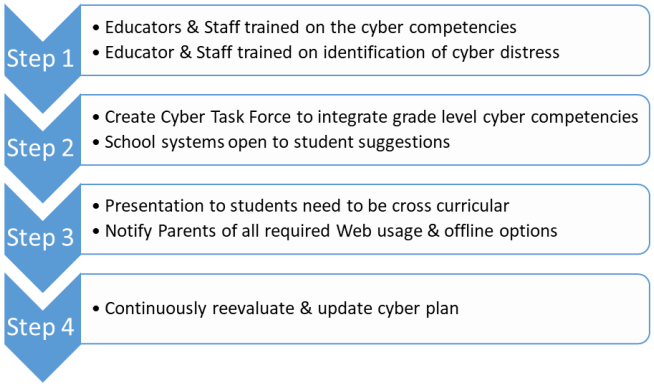

Figure 5. Solution Model [12].

Step one is the most time consuming and difficult as it involves training and convincing educators and staff to change the way they think about cyberbullying and being open minded. For example, do not share students' personal information with third party vendors for classroom tools. Educators and staff need to be trained on the cyber competencies, how to apply the cyber competencies, and actions that should be taken when dealing with students in cyber distress. An example of a good training program is the First Bytes Academy that Lord Fairfax Community College in Virginia has. In First Bytes Academy, educators and staff learn the four main competencies through classroom lectures and hands on activities. During the academy, educators and staff work with students so that they can practice different techniques for teaching the cyber competencies to their students. The First Bytes Academy teaches the two additional cyber competencies to those educators and staff who are at schools that would need them. Also, the First Bytes Academy has professionals come and train the educators and staff on how to properly handle cases of cyber distress.

Step two requires support from administration and collaboration between school system IT staff, educators, and students. The cyber taskforce should actively be sharing cyber competency resources with all members of the K-12 community. By sharing the cyber competencies with the entire K-12 community there will be more people aware of the different causes of cyber distress so they will be more active in protecting their information and more aware if the signs of cyber distress. The cyber taskforce is comprised of administrators, educators, staff, and students from the school district. The cyber taskforce is to work together and integrate the cyber competencies into the already existing curriculum for each grade level. This process will seem time consuming, but once you figure out how to integrate it at one grade level you can replicate it at another just with either a higher or lower degree of difficulty.

Step three is presentations have to be relevant and relatable at a local level. For example, have a local cyber victim speak or have a student panel allowing students to express their concerns. The in school presentations should be one of two ways. The first way is bringing in a professional from the area who has a personal experience with cyber distress and someone the students can relate to. The second way is to have student panels where students can share their experiences with cyber distress and share with the school how they think they could help those in cyber distress. The out of school presentations involve partnering with organizations such as the Girl Scouts, the Boy Scouts, the Moose, and the Elks. The school partners with these organizations and hosts events or presentations for them in which the students at the school teach the cyber competencies to the community. This allows school administration to ensure students are understanding the cyber competencies and students are teaching their peers which Generation Z and Alpha are more willing to learn from. Also, during this step school administration needs to be actively informing parents about all of the web usage that their child is being required to do for school. The parents also need to be informed of the offline options for the web usage in case the parents do not feel that it is safe for their child to be using certain tools online.

Step four is important to ensure that cyber education at the K-12 level is successful. The cyber plan needs to continuously be reevaluated and updated to stay current with modern technology and generational times. For example, many school systems are still focusing on what Generation Y needed instead of Generation Z and Alpha demands. The cyber taskforce should constantly be collecting feedback from educators, staff, administrators, parents, and students about the integration of the cyber competencies into the curriculum. If a component of the cyber competencies is not being perceived well, then the cyber plan needs to be reevaluated to have that component incorporated in a different way.

Many organizations are trying to aid in the effort of educating through the cyber competencies. Some of the organizations that are the most active in educating through the cyber competencies are the Safe Surfin' Foundation [15], Bikers Against Child Abuse [3], National CyberWatch Center [9], Internet Safety 101 Organization [8], and StopBullying [16].

Incorporation of cross-curricular cyber problems leads to students that are actively engaged in solving the problems. Educators and staff are more competent in the CIA (Confidentiality, Integrity, Accountability) Triad and can encourage student learning beyond a canned lesson plan to produce better mastery of and interest in computer science and cybersecurity. This method focuses on the outcome of increasing the number of computer science and cybersecurity professionals while keeping students involved and providing a solution that they can have a voice in. Educators are held accountable for understanding the risks involved with using free tools just because they are cool. Finally, this method is a source of open communication and partnership between K-12 school systems, higher education institutions, computer science organizations, and cybersecurity organizations.

 ISBN: 978-1-61208-764-1

V. CONCLUSION

Frederick County Public School System in Virginia, USA and Texas Public School System in USA have found a decrease in K-12 cyber distress and an increased interest in computer science and cybersecurity courses as a result of using this model. To ensure that K-12 and higher education expectations are in line, community college professors should serve on K-12 program advisory boards and K-12 representatives should serve on the community college curriculum advisory committee. Community colleges that take this approach have found that it has allowed for open discussions on how to better connect K-12 computer science and cybersecurity courses to community college computer science and cybersecurity courses.

In conclusion, my efforts to improve K-12 cyber education and increase cyber enrollment has evolved through national organizations, such as Safe Surfin' Foundation by providing speakers at schools and educational materials. Early parts of this model have been vetted by inclusion in the National CyberWatch's 2017 [11], 2018 [10], and 2019 [13] Innovations in Cybersecurity Education. Also, parts of this model have been vetted through the National Center for Women & Information Technology (NCWIT) AspireIT Grants and Aspirations in Computing (AiC) awards and Girls Scouts USA Gold Award. Other parts of this model have been supported by research presented at the 2019 Federal Partners in Bullying Prevention (FPBP) Summit on Cyberbullying Prevention. This solution was initially presented at the 2019 Association for Computing Machinery (ACM) Special Interest Group on Computer Science Education (SIGCSE) [10] and updated model presented at the 2019 Community College Cyber Summit (3CS) [11]. This solution continues to evolve into a duplicable K-12 to higher education cyber curriculum model that engages students in cyber at the elementary school level to high school seniors, so that they will want to continue in the field.

REFERENCES

[1] V. Johnson, "A Lifetime Promise: The Amanda Straubs Story," 2014.

[2] About CSForAll. Retrieved August 2, 2020, from CSForAll: https://www.csforall.org/about/.

[3] Bickers Against Child Abuse. Retrieved November 14, 2020 from: https://bacaworld.org/.

[4] M. Bishop, S. Buck, D. Burley, J. Ekstrom, L. Futcher, D. Gibson, E. Hawthorne, S. Kaza, Y. Levy, H. Mattord, and A. Parrish "CSEC2017," ACM, IEEE-CS, AIS SIGSEC, & IFIP WG, 2017. DOI: 10.1145/3184594. Retrieved November 1, 2020 from: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.

[5] Finding Faith. 2013. Retrieved November 14, 2020, from IMDb: https://www.imdb.com/title/tt2201760/.

[6] M. Geissler, C. Servin, M. Stange, C. Tang, and C. Tucker, "Cyber2yr2020," Association of Computing Machinery (ACM) Committee for Computing Education in Communty Colleges (CCECC), 2020. United States. DOI: 10.1145/3381686. Retrieved November 1, 2020 from: http://ccecc.acm.org/files/publications/Cyber2yr2020.pdf.

[7] E. Hawthorne, T. Moore, C. Servin, C. Tang, and C. Tucker, "CSTransfer2017," Association of Computing Machinery (ACM) Committee for Computing Education in Community Colleges (CCECC), 2017. United States. DOI: 10.1145/3108241. Retrieved November 1, 2020 from: https://ccecc.acm.org/files/publications/CSTransfer2017.pdf.

[8] Internet Safety 101 Organization. Retrieved November 14, 2020 from: https://internetsafety101.org/.

[9] National CyberWatch Center. Retrieved November 14, 2020 from: https://www.nationalcyberwatch.org/.

[10] R. Stange, "Cyber Tween," National CyberWatch 2018 Innovations in Cybersecurity Education, p. 61, 2018.

[11] R. Stange, "A High School Sophomore and CSTA Cyber Teacher Leads Her Peers In Day of Cyber," National CyberWatch 2017 Innovations in Cybersecurity Eductaion, p. 42, 2017.

[12] R. Stange, "Increase K-12 Cyber Competency to Prevent Cyberbullying," Association of Computing Machinery (ACM) SIGSCE, 2019.

[13] R. Stange, "Increase K-12 Cybersecurity Competencies to Increase Cybersecurity Enrollment," National CyberWatch 2019 Innovations in Cybersecurity Education, p. 59, 2019.

[14] R. Stange, M. Stange, and H. Coffman, "Increasing K-12 Educator Knowledge to Prevent Cyberbullying & Enhance K-12 Cybersecurity Courses," Community College Cyber Summit (3CS), 2019.

[15] Safe Surfin' Foundation. Retrieved November 14, 2020 from: https://safesurfin.org/.

[16] StopBullying. Retrieved November 14, 2020 from: https://www.stopbullying.gov/.

 ISBN: 978-1-61208-764-1