

TEACHING CYBERSECURITY IN K-12 SCHOOLS

by

Kharyssa Pye

A Capstone Project Submitted to the Faculty of

Utica College

August 2016

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Cybersecurity

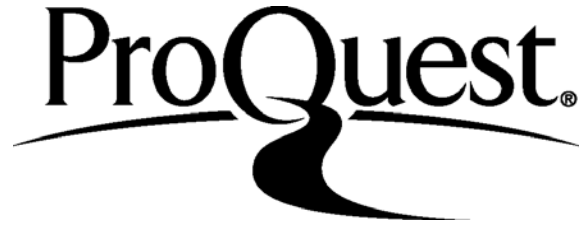
ProQuest Number: 10155676

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



ProQuest 10155676

Published by ProQuest LLC (2016). Copyright of the Dissertation is held by the Author.

All rights reserved.

This work is protected against unauthorized copying under Title 17, United States Code
Microform Edition © ProQuest LLC.

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

© Copyright 2016 by Kharyssa Pye

All Rights Reserved

Abstract

This project focused on the teaching of cyber security in k-12 schools. The specific areas of interest were on the education of C3 content to children and young people through the education systems. In this paper, I discuss the challenges and situations that necessitated teaching of cyber security in k-12 schools. Cyber crimes and attack are among the most common ills devised by some computer experts. These crimes take various forms; espionage, forgery, cyber stalking, impersonation, virus attacks, email bombing, and so on. These attacks affect children and young people just as much as it affects adults. If anything, children are more vulnerable than adults because most of them are not able to identify potential threats in the cyber space. Some young people also perpetrate cyber crimes such as cyber bullying because they do not have knowledge of cyber ethics. The main finding was that C3 content had not been effectively delivered in k-12 schools, due to a number of reasons. Part of the reason is that k-12 schools have not fully integrated the subject into their curriculum as a course to be studied. The educators are also not sufficiently equipped to teach C3 content in their respective schools. This paper recommends that the state department of education is working together with district officials develop a proper policy framework to oversee the implementation of cyber security in the curriculum of k-12 schools. Also, professional development training on C3 content should be offered to educators who will deliver the concepts to their students. Keywords: Cyber Security, Professor Christopher Riddell, CyberSmart, Stop.Think.Connect, StaySafeOnline.org, NetSmartz, and cyber bullying.

Acknowledgements

I would like first to thank my Lord and Savior Jesus Christ, for without him the journey to obtain my Master's Degree would not have been possible. I would also like to thank Professor Christopher M. Riddell and my second reader, David Plude, for their advice and assistance to make this report a success.

To my family and friends, thank you for helping me and comforting me through my time of struggle. Thanks for your motivation and willingness to sacrifice for me.

To my son, Deramous Cordell Harris, Jr., aka "DJ," this is dedicated to you little guy! You are my inspiration, my drive, and my will to live. If I do not do anything else in life, at least I know I made you proud.

Table of Contents

List of Illustrative Materials.....	vi
Teaching Cybersecurity in K-12 Schools	1
Literature Review.....	5
Current School-Based Strategies	7
Impediments to the Formation, Adaptation, and Implementation of a Curriculum.....	15
Factors that Limit the Use of School Curricula	21
Discussion of the Findings.....	26
Recommendations.....	32
Future Research	41
New Research Question 1	41
New Research Question 2.....	43
New Research Question 2.....	43
References.....	45

List of Illustrative Materials

Figure 1: CyberSmart K-12 Keep It Private Worksheet.....	9
Figure 2: Stop.Think.Connect Educational Poster.....	10
Figure 3: StaySafeOnline.org Middle/High School Lesson Plan	12
Figure 4: StaySafeOnline.org Middle/High School Lesson Plan (continued).....	13
Figure 5: Image on Danielle Deep’s Facebook page	15

Teaching Cybersecurity in K-12 Schools

As emphasized by Rowe, Lunt, and Ekstrom (2011), our world has now moved into the digital realm where computers and the Internet have become an integral part of everyday life. In the past, computers were used for the purpose of entertainment and played other minor roles that would not have put its users at risk. However, as technology advanced, high-tech machines are being used for a lot more than just play. Along with these changes are equally outrageous threats and an unprecedented rise in cyber crime rates. As pointed out by Aloul (2012), the increased usage came with risks that potential users had to manage. The Internet has now become a hub where a variety of activities, such as socializing and making purchases, take place. They have become a central part of people's lives. As a result, it is prudent to address some of the risks users expose themselves to.

The virtual world epitomizes an environment where there may be a greater license to participate in unjustified behavior because of the anonymity and the ability to mask one's identity. Students need to be cognizant and understand that there is no such thing as perfect security. Prohibited cyber attacks come through the establishment of protection strategies and education. Cyber security is one of the key issues that computer users need to know and one of the most critical economic and national security challenges we encounter as a nation. Enlightening the public on how to remain safe in the cyber world is a key necessity. In the past, the issue had only affected governments and large corporations. However, more than 3 billion people are now using the computer more frequently and the Internet for more tasks (Davidson, 2015). One reason Internet access has surpassed over the past 15 years is the rising affordability and availability (Davidson, 2015). As cited in Lestch, the executive director of the National Cyber Security Alliance, Michael Kaiser stated, "Using technology is one of the three 'Rs' of the

21st century.” He further proclaimed, “If you do not graduate from high school knowing how to use technology, it is going to be a hindrance in the same way if you do not know how to read” (2015). The three R’s are referencing the traditional subjects of reading, writing, and arithmetic.

The purpose of this research was to examine the need for cyber security education implemented in classes to children in the k-12 school curriculum. What are the curricular approaches or school-based strategies tried in teaching cyber security, safety, and ethical conduct in k-12? What are some of the impediments to the formation, adaptation and implementation of a curriculum that addresses cyber security? How can the factors that limit the use of school curricula in combating cyber security be surmounted?

Since computers are now ubiquitous, and cyber security is unreserved for government and large corporations, it is important to make the public aware of the matter so that they can increase their response to the issue. Introducing a curriculum that addresses cyber security as a critical area of learning through all the stages, should be the ideal focus of the government and educators. As argued by Niekerk, Reid, and Thomson (2013), teaching cyber security from an early age is the best possible way of improving its awareness among the public. Several reasons support this approach. The public can easily appreciate the importance of the matter if enough effort is made to teach them from an early age. For example, children taught about cybersecurity throughout their k-12 school program will be able to recognize the issues as an integral part of their lives and use the knowledge gained to practice safe use of the computer and the Internet (Neikerk, Reid, & Thomson, 2013). By making such a study a component of the contemporary education, it will help them grasp its importance.

The need for cyber security education in public and private institutions is directly related to the growing threat landscape. The main challenge with creating cyber security awareness

among people is convincing them that their little actions can jeopardize information security on a larger scale (Niekerk & Solms, 2013). For example, some individuals only use the computer and the Internet as a socialization tool. These people interact with each other online, assuring themselves that their reduced use of a computer does not put them at risk. However, making cyber security part of the curriculum in k-12 schools serves to remind these adults that it is a crucial thing that needs addressing at all levels (Niekerk & Solms, 2013). Cyber security awareness will help individuals reduce vulnerabilities and expose them to potential cyber attacks. Making people aware is only possible when the individuals believe that there is a need for them to learn such knowledge.

Moreover, online criminals have gained substantial notoriety in the recent past and are now more capable of launching devastating attacks. The quest to protect all digital life on the internet begins with the ability of normal people to detect such attacks and launch counterattacks to diffuse the threat and maintain computer and online security (Pfleeger & Caputo, 2012). The number of individuals capable of identifying basic attacks and reacting to them before they cause harm is related to how well cyber security issues prioritized among the population.

At present, universities are where most students become exposed to the subject for the first time in their lives. Children today are using the immense power of digital media to discover, associate, form, and learn in ways never been conceived. They are isolating themselves from traditional communication methods and substituting them with instant and text messaging, keeping their friends posted on their daily activities and whereabouts with social networking. They also play games against people across the globe and use the Internet to find and play music and watch movies and television with this power. Children of all ages have unlimited

opportunities; yet, they face potential pitfalls, such as cyberbullying, sextortion, cyber drug trafficking, and cyberstalking, and other safety and security concerns.

Introducing cyber security as a critical learning element in lower schools will enable cyber security professionals of the future to be more competent and allows them to be ready to identify vulnerabilities and react to them. For example, introducing the topic in k-12 education program will increase its awareness among the young population. As a result, there are those who will develop an early interest in the subject and will be more competent in tackling cyber security issues since they have received exposure at a very young age (Ekstrom, et al., 2011).

Indicating some of the benefits that will accrue from introducing such a program at the lower levels of education is also imperative. First, the children will be able to appreciate cybersecurity as an important issue that affects their lives when they are using computers and the Internet. The children will be motivated to take a personal initiative to protect themselves from cyber crimes because they will gain a deeper appreciation of how the threat is constantly present in their lives. Additionally, addressing cyber security issues from the lowest levels increases the prospects of fighting attacks at the higher standard (Pfleeger & Caputo, 2012).

Due to the interconnectedness perpetuated by the Internet and the pervasive use of the computer, an individual on a network acts as a potential entry point to a host of other persons sharing a network. Such as, the cyber attacker has been known to identify potential vulnerabilities in users of a network to determine a point where they can launch an attack that will spread to the whole ecosystem. The vulnerability can come in the form of a bug in a program or an individual with poor cyber security information who can be exploited to launch an attack on the rest of the members (Aloul, 2012). Teaching children to be aware of the threats

they are exposed to when using computers and the Internet makes them conscious of their activities and lessens the possibility of cyber attackers using them as a weak link.

In the past, it has been the norm by cyber attackers to use one individual's computer to spread wrong information and programs over a network. If individuals are made more security conscious, there will be fewer incidences of people being exploited by attackers to carry out large-scale cyber attacks (Ekstrom et al., 2011). As a result, teaching children and the general public to be aware of such issues from an early age increases the prospects of winning the war against cyber crime and promoting cyber security.

Introducing a curriculum on cyber security from the low levels of education is also important. The k-12 educational attainment is one of the best targets, simply because students learn about computers and their use at that level. It is the lowest level that students can be able to appreciate the weight of the matter and develop an interest in promoting cyber security both in their personal lives and to the general public. The success of the program will see it being extended to other levels of education and create a form of continuity that links it to current information security services offered at the college level and the university (Ekstrom, et al., 2011). It will generate more awareness in both the students and the general public and promote security in using computers and the Internet. However, for most school districts, outdated infrastructure will present a challenge because it cannot support the demands of classroom technology.

Literature Review

Technology has brought a huge number of benefits to the educational community, including enhanced access to information, productivity, better simulation capabilities, and ways to provide technology-based support. Despite this progress, technology has also been associated with

significant challenges. In 2008, a survey was conducted to explore the nature of Cyberethics, Cybersafety, and Cybersecurity (C3) educational awareness policies, initiatives, curriculum, and practices currently taking place in the U.S. public and private k-12 educational settings. The survey found the state of C3 Education to be incomplete (Pruitt-Mentle, 2008). Per the study of Pruitt-Mentle, C3 content was limited, educators did not feel comfortable with the topics, and standards for the content only marginally discuss the issues (2008). Data from the survey also revealed the majority of the responsibility for transmitting C3 content to the students was in the hands of the educators; yet, in theory, the content is not mandated, and teachers feel unprepared to teach the topic (Pruitt-Mentle, 2008). 67% of respondents reveal they do not know how to update anti-virus, spyware, and anti-spam filters, and 52% do not know how to install operating system patches. Over 25% are not at all prepared to discuss basic Cybersafety issues, and amazingly, 75% of educators feel uncomfortable discussing topics that have had significant public attention, like cyberbullying (Pruitt-Mentle, 2008).

Laws and professional educational standards regarding C3 in k-12 schools guide teacher practice. According to an article in *Journal of Digital Learning in Teacher Education* written by Portia Pusey and William A. Sadera, two federal laws, in the past two years were approved that modified k-12 education (2011). The Children's Internet Protection Act (CIPA) forces schools to have a clear Internet safety policy. The policy was established to protect students from contact with offensive content through the use of Internet filters. The Broadband Data Improvement Act (2008) requires schools to teach proper online. The National Educational Technology Standards (NETS) also mandates that C3 content is taught in schools. However, these laws and requirements are broad and unclear in their strategy and suggestions (Pusey & Sadera, 2011, p. 82).


According to the 2011 United States Department of Education report, students that enter their freshman year of college have used computers in the past, and some of them are very proficient in their usage. There are many programs devoted to teaching computer security to professionals and members of the private sector; yet, there are minimal attempts to target the younger audience. The National Cyber Security Alliance (NCSA), sponsored by Microsoft Corporation, finds that schools are ill-prepared to teach students the basics of online safety, security, ethics, and skills that are essential in today's digital times. It advocates for a comprehensive approach to teaching online safety, security, and ethics to be part of k–12 education nationwide (U.S. Schools not preparing kids for digital age, 2011). A program that can teach children and teachers the basic tenets of cyber security would set the standard for cyber security curricula. Some notable examples of k-12 curricula and school-based strategies are noted below.

Current School-Based Strategies

CyberSmart

CyberSmart is the first online professional development that provides educators with a hands-on experience to meet the learning needs of today's students. CyberSmart Africa reaches out to the deprived schools, with the world's first adapted interactive whiteboard operating with cheap solar power. www.cybersmart.orgwww.cybersmartafrica.org. The CyberSmart Learning Platform sets the world's most progressive learning technologies, quality content, and training into a single mobile unit. The platform contains an Android computer, an energy-efficient super-bright projector, interactive whiteboard capabilities, solar rechargeable batteries, speakers loud enough for classroom use, advanced 3-D capability, cooling fans, and a unique dust filtration system. All packaged in highly durable aluminum unit, it moves quickly between classrooms impacting hundreds of student in a single day (National Cyber Security Alliance, McAfee, and

CyberSmart! Education Team Up to Bring Cybersecurity Learning Resources to K-12 Classrooms, 2016). CyberSmart also provides teachers with Common Sense Education's K-12 Digital Citizenship Curriculums that they can use to help form a positive school culture in the classroom that supports the safe and responsible use of technology. It gives students the opportunity to build skills around critical thinking, ethical discussion, and decision making. It also allows the students to connect with other students across the globe by getting recognized for their efforts (National Cyber Security Alliance, McAfee, and CyberSmart! Education Team Up to Bring Cybersecurity Learning Resources to k-12 Classrooms, 2016). CyberSmart is very comprehensive and utilizes a variety of media and teaching modes. The website includes lessons plans, with activities like classroom discussions, safety games, and tip sheets. Figure 1 shows an example of a privacy k-12 worksheet called "Keep it Private." The worksheet is provided to educators through CyberSmart.

GRADES K-2
Keep It Private 

*** DID YOU KNOW ...**
 Privacy matters to everyone! In Spanish, the word "privado" means private.

Match the words to their definitions

Internet	something that you should keep to yourself, or share only with people you trust
credit	a piece of work that is new and created firsthand
private	an electronic system that connects billions of people using computers, phones, or other devices, and allows them to communicate with one another
original	public acknowledgement or praise given to a person

*** WHAT DO YOU THINK?**
 When might you be asked to give out private information on the computer?

*** DO YOU REMEMBER ...**
 What kinds of information you should keep to yourself when you use the Internet?

1. Family Activity
 Help a parent come up with a safe username to use on the Internet! To help your parent pick a username, find out:
 1) his or her favorite pet or animal,
 2) a favorite TV show, book or movie, and 3) his or her favorite numbers. Use the information to make a username and then double check that you followed all the "Common Sense" rules so that the username is safe and secure.

2. Tech It Up!
 With a parent or family member, visit a website such as Eekoworld (<http://pbskids.org/eekoworld>) and sign up using a secure username that you pick together. (Note: On Eekoworld, the sign-up button is in the upper left corner if you're staring at your computer screen!) Adults: You can use any site that you want for this activity, but we recommend sticking to a non-commercial website.

3. Common Sense Says ...
 Many websites require you to create a username. A username is like a code name that you give yourself when you're using the Internet. Never include any private information in your username, such as your real name, age, birthday, the name of your school or hometown, or parts of your address or phone number.



 WORKSHEETS / REV DATE 2015 / www.common sense.org/educators
 CREATIVE COMMONS. ATTRIBUTION-NONCOMMERCIAL-SHAREALIKE 

Figure 1: CyberSmart K-12 Keep It Private Worksheet

Stop.Think.Connect

Stop.Think.Connect is a national public awareness campaign created in 2010 to heighten the understanding of cyber threats. This campaign empowers the American public to be safer and more secure online. The Stop.Think.Connect campaign is not a curriculum but an initiative to spread information about Internet safety. Brochures, tip sheets, and other quick resources for children and parents are found on the website. Federal government training programs are also available with this campaign (National Initiative for Cybersecurity Careers and Studies (NICCS), n.d.). This campaign is not just a curriculum but an intuitive to spread information about Internet safety. The website provides quick reference resources, posters, and tip sheets for teachers,

students and parents. Figure 2 shows an example of an educational poster provided to educators through Stop.Think.Connect. The poster signifies online bullying and encourages people to be good citizens online. It describes how people should only post things about others, unless they would want the same thing in return.



Figure 2: Stop.Think.Connect Educational Poster

StaySafeOnline.org

StaySafe.org is a program created by the United States' National Cybersecurity Alliance. The program is dedicated to “educate and empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals use, the networks they connect to, and our shared digital assets” (New York Internet Crimes Against Children Task

Force, 2012). The program provides teachers with three different teaching materials and lesson plans created for various age groups k-2nd grade, grades 3-5, and middle and high school. Each age group has a different set of learning objectives, which include scenario discussions, classroom activities, and games to illustrate cyber concepts (New York Internet Crimes Against Children Task Force, 2012). It is designed to assist teachers with basic tips for keeping students at all levels engaged and help educate students at all levels to understand and apply to their online experience. Different sets of teaching materials were established on this website for different age groups k-12, 2nd grade, grades 3-5, and middle and high school. The website provides each age group with different set of learning objectives. Figure 3-4 shows a lesson plan for middle and high school students provided to educators through StaySafeOnline.org.

DATE: Fall 2009	GRADES: Middle School / High School Levels
PROGRAM: National Cyber Security Alliance Volunteer Project	SUBJECT: Language Arts
TOPIC: Becoming Smart Digital Citizens~Using the C3 Concepts and WWW Checklist!	MATERIALS: <ul style="list-style-type: none">• Volunteer Packet Including: Teacher Tip Sheet, Parent Tip Sheet, Homework Assignment, Answer Sheet• Chalk or Markers for Board• Team Recorder will need a pencil
TIME DURATION: 60 Minutes	

OVERALL LESSON CONTENT:

Students will be introduced to the C3 Concepts and WWW Decision Tool and asked to use them to solve scenarios involving typical cyber issues their age group faces.

WHAT IS THE OVERALL PURPOSE OF YOUR PRESENTATION AND ACTIVITIES?

Students will gain an understanding of the C3 Concepts and how they can apply these to their regular online use.

Students will understand how to use the WWW Decision Tool to make wise decisions about sharing information online.

WHAT SHOULD STUDENTS BE ABLE TO DO WHEN YOU ARE DONE TEACHING CONCEPTS?

Students will incorporate the C3 Concepts and WWW Decision Tool into regular online activities.

Students will work in small groups to critically analyze the missteps many of the individuals in the scenarios made and will use the new concepts learned to help them navigate these online experiences better in the future.

Students will be able to work independently to complete homework assignment and practice concepts learned through whole group and small group lessons.

GETTING STARTED- STEPS TO COVER CONCEPTS AND COMPLETE ACTIVITIES TIMELY.

Introduction (whole group)

C3 Concepts & WWW Decision Tool- Becoming A Smart Digital Citizen Lesson (whole group)

Team Reinforcement Lesson (small group)

www.staysafeonline.org

Figure 3: StaySafeOnline.org Middle/High School Lesson Plan

Independent Practice (Take home assignment)

HOW WILL YOU KNOW STUDENTS UNDERSTAND THE CONCEPTS YOU ARE TEACHING?

During whole group lesson- How are students categorizing online activities on the brainstorm list. (If they don't seem to understand, briefly explain concepts again.)

Small group activity-Walk around as groups work. Listen to student participation. If they seem to be struggling, give prompting clues to get them back on task.


Figure 4: StaySafeOnline.org Middle/High School Lesson Plan (continued)

NetSmartz Workshop

NetSmartz Workshop is an interactive, educational program of the National Center for Missing & Exploited Children® (NCMEC) that provides age-appropriate resources to aid with teaching children how to be safer online and offline. The workshop is for children ages 5-17, parents and guardians, educators, and law enforcement. With resources such as videos, games, activity cards, and presentations, NetSmartz entertains while it educates. The NetSmartz Student Project Kit helps students in grades 6-12 teach their peers and younger students about topics like

cyberbullying, online privacy, and digital ethics. The workshop provides teachers with a free collection of online resource materials for primary, intermediate, middle school, and high school grade levels to help them create a dynamic Internet safety curriculum (NetSmartz Workshop, n.d.). Netsmartz uses a variety of teaching materials for subtopics such as videos, activity cards, teachable recipes, safety presentations, handouts/activity worksheets, and safety rules. Figure 5, “Stand by or Stand up” worksheet, shows an educational interactive comic worksheet for intermediate and middle school students provided to educators through NetSmartz Workshop.

STAND BY OR STAND UP ?



SUGGESTED GRADES
Intermediate and Middle School

INTERNET SAFETY ISSUES
Cell phones
Cyberbullying
Social networking

INSTRUCTIONS
Have students play the interactive comic - *Stand By or Stand Up?* on NSTeens.org. Then, use this discussion guide to help them better understand the comic's lesson.

RELATED RESOURCES

- » Video - "Terrible tExt"
- » Video - "Cyberbullying"
- » Intermediate Pledge

DISCUSSION QUESTIONS


1. **How do you think Katie felt when her picture was being passed around?**
Katie probably felt sad, embarrassed and alone. She might not have wanted to come to school because her classmates were the ones bullying her. Katie might have also felt afraid to tell an adult, like her parents or a teacher, because she thought no one could help.
2. **Why do you think so many people joined in the cyberbullying?**
A message or picture being passed around is like a snowball – it starts out small, but it quickly gets bigger and bigger. Once Katie's picture started being passed around, it was hard to stop. Some people who joined in probably thought they were just being funny by passing the picture around. Some people may have felt pressured to join in because their friends were doing it. Some may have not liked Katie and wanted to be mean to her.
3. **There are several times during the comic when you have to make a choice. Which path did you choose and why?**
First choice: Send the picture to John or don't send it?
Second choice: Forward the picture or delete it?
Third choice: "Like" the page or report it?
Fourth choice: Help Katie pick up her books or walk away?
Fifth choice: Lie to the teacher or tell the truth?

Encourage students to imagine what would have happened if they chose differently. You may even want them to play the comic again to make different choices.
4. **What else could you have done to help Katie?**
You could have shown Katie that you support her by being her friend, sending her a nice message, walking with her in the hallway, or sitting with her at lunch. You could have told the cyberbullies to stop; John is your friend and may have listened to you. You could have also told an adult about it, like your parent or a teacher. An adult could have talked to the cyberbullies and gotten them to stop.
5. **Why should you speak up and not stand by when you see someone being cyberbullied?**
If you see someone being cyberbullied and ignore it, you are being a bystander. Bystanders are sometimes afraid to say something because they think they will be cyberbullied, too. They might also think that adults can't help or that they'll be seen as a tattletale. But bystanders actually have a lot of power. If no one ever steps in to tell cyberbullies that what they are doing is wrong, then they will just keep cyberbullying. If you stand up to them, you can help someone else from being hurt.

Watch videos and play games at
NSTeens.org

NetSmartz Workshop

A program of the



NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

Copyright © 2013 National Center for Missing & Exploited Children. All rights reserved. Animated Characters Exploding Ted Copyright © 2005-2013 National Center for Missing & Exploited Children and Boys & Girls Clubs of America. All rights reserved.

Figure 5: Image on Danielle Deep's Facebook page

Impediments to the Formation, Adaptation, and Implementation of a Curriculum

A Missouri state accountant, Ms. Galloway, conducted a review dubbed 'Cyber Aware Schools Audits', of the existing cyber security measures in five districts spread within the

country. Her report revealed some current realities when considering implementing a cyber-security conscious k-12 curriculum, as these realities could serve as obstacles or could drag the process. Ms. Galloway also brings to our attention some stakeholders who would prove useful in pushing through with such an initiative, notably, the district official in charge of technology and k-12 district representatives. According to the study, if awareness is not addressing these issues at a higher level of authority, then little success can be anticipated at the school level (Doran, 2016). The report noted the following existing challenges, which in one way or another impact the efforts of developing a cyber-security aware curriculum:

1. There was no data governance plan in place.
2. There was no IT security administrator whose sole responsibility was ensuring the safety of the infrastructure and resources of IT within the district.
3. There were no processes in place to prevent simultaneous session logins, and neither was there one to govern password changes.
4. Staff members did not have a security awareness program that they could follow
5. The practices of the vendors were not adequately monitoring Internet activity.
6. Lastly, there was no plan of action with regards to what the district and its officers would do if a crippling cyber-attack or data breach happened (Doran, 2016).

The head of a consulting group within the state, Doug Levin, also noted that state divisions of education would be undertaking much more to create rules for k-12 systems' data security besides implementing them, up front (Doran, 2016). He added that another challenge was that nearly 50% of districts nationwide did not have a dedicated IT professional on staff, and those that did characteristically face budget constrictions (Doran, 2016). As noted by other privacy advocates that attempted to address these issues, more comprehensive and sustained

efforts at the state and local level are needed (Doran, 2016). Doran's report also proclaims a lack of cyber security awareness amongst state officials was also necessary when a review of the student data practices by the state's education department, revealed that they were collecting student's social security numbers without the need for them and their unpreparedness to handle a major data breach (2016). Also, some k-12 district officials were noted to have concerns over the possible implicit costs that could result from taking steps towards improving the state of cyber security within the district schools. More so, some state staff found extra security measures annoying, which Doran's report noted that could be expected, as tightened security would consequently mean increased complexity (2016). Another challenge is that even though some district officials may have begun taking steps towards preparing themselves for a cyber-attack, such measures remain undocumented (Doran, 2016).

School management, k-12 district officials, and state department of education staff that are cyber-security literate appreciate the need of having such knowledge imparted on k-12 students (Computer Science Teachers Association, 2003). As noted in the *Model Curriculum for the k-12 Computer Science Report*, "Due to an absence of standards, teachers graduating from colleges of education have not typically been well prepared to teach computer science" (Computer Science Teachers Association, 2003). The report also states, if they hardly ever implement even the most basic cyber-security measures, it would be difficult to expect them to introduce such a topic to their students; because it comes as no surprise that few would advocate for its inclusion in the school curriculum (Computer Science Teachers Association, 2003).

The existing status quo is already a hindrance in itself, since people and institutions alike are always initially resistant to any manner of change, particularly when many uncertainties present themselves, as would be the case with a cyber security inclusive curriculum. According

to a survey of 1,000 adults in the United States aged 18 – 26 years in 2014, a shocking 64% of the respondents specified that they had not taken any computer classes in their high school education that would have equipped them to take up cyber careers. This included computer science (Raytheon in conjunction with the National Cyber Security Alliance, 2014).

National Cyber Security Alliance feels the dynamic nature of cybersecurity and what is relevant today may not be pertinent a few months from now (Raytheon in conjunction with the National Cyber Security Alliance, 2014). Over the past many years, the existing k-12 school curriculum has undergone little change, which has made its implementation easy. However, introducing a knowledge area like cyber-security into the curriculum will only increase the complexity of defining such a school curricula as new cyber-threats and remedies are being discovered on a near daily basis (Raytheon in conjunction with the National Cyber Security Alliance, 2014). One question the National Cyber Security raises is how quickly the curriculum can adapt to such rapid changes (Raytheon in conjunction with the National Cyber Security Alliance, 2014)?

The National Cyber Security strongly feels the other challenge lies in the complexity of cyber security as a subject in itself. They believe the following questions then need to be addressed: What is relevant for each grade? How do we simplify the content for the lower level children to grasp best the cyber-security concerns that could affect them at their level? How much is enough for teaching at the k-12 level and what can be left for higher level teaching in colleges and campuses (Raytheon in conjunction with the National Cyber Security Alliance, 2014)? For as it stands, most formal training on cyber-security begins at the college level, with the majority of the students taking the course having had no prior interaction with such information, according to the National Cyber Security Alliance (2014). They go on to further

state, at the college level, much information is compressed in a single learning unit in an attempt to cover all the aspects of the discipline (Raytheon in conjunction with the National Cyber Security Alliance, 2014). They further state this makes learning harder for college and campus level students difficult, as they are expected to familiarize themselves quickly and efficiently with and understand and apply many cyber security concepts all within a limited span of time. As might be expected, only the exceptional students and those who had an opportunity to interact with the disciplines of cyber security at an early age can excel under such immense pressure (Raytheon in conjunction with the National Cyber Security Alliance, 2014).

Raytheon jointly with the National Cyber Security Alliance, also state the failure by school management and state education departments in acknowledging the piqued interest in the field of cybersecurity by most Millennials and younger generations is another unique challenge that needs overcoming (2014). Per the National and Cyber Security Alliance, this could probably be achieved by exposing kids from elementary school age to the various aspects of cyber security. It would involve teaching them about the importance of privacy on the web, ways of protecting web resources online, and so on (Raytheon in conjunction with the National Cyber Security Alliance, 2014).

In an article written by Corrine Lestch, she suggests a failure of properly having cyber security defined as a career (2015). She believes this has a trickle-down effect, as it will be noted that throughout a child's academic life, one will rarely hear a teacher or career mentor advise them to consider cyber security as a possible career option, as compared to other career options present (Lestch, 2015). This unfamiliarity with the field until one's college years already presents a hurdle for the college student in considering taking up cyber-security as a course they can pursue and later consider seeking employment in the same field. If students are introduced to

cyber-security early enough; just as many schools worldwide introduce students to computer programming at a young age, the interest in pursuing the branch of IT as a career will grow. Even so, there has to be goodwill from educationists and policy makers (Lestch, 2015).

Another issue that could be further complicating the effort of having cyber-security adopted in the school curricula is failing to approach the issue from a school district perspective (Niekerk & Solms, 2013). If school district administrators joined efforts in advocating for the inclusion of cyber-security in the curriculum, then they would have a much stronger voice. This challenge presented itself when "... an experienced external hacker seized the computer systems at Swedesboro-Woolwich School District and held them for ransom – making it incredibly difficult for kids at four primary schools to do their web-based statewide examinations as scheduled" (Niekerk & Solms, 2013). The interim superintendent of the school district admitted to not having anticipated such an attack, as the general assumption has been that only government institutions and other large organizations need to worry about such attacks. Therefore, other school district administrators can learn from such an event and not only secure their school district networks but also site such scenarios as evidence for the need to have cyber-security included in the curricula (Niekerk & Solms, 2013). Collaboration and coming together enhances the chances of being heard by those that can affect the necessary changes in the school programs. More so, this applies to public schools where changes cannot just initiate without approvals from the powers and officers who make the decisions (Niekerk & Solms, 2013). Niekerk & Solms suggests some laws and regulations have to be followed for things to happen in such schools (2013).

The other difficulty lies in the challenge that many other disciplines have now become of national and international concern could also be competing for inclusion in the k-12 school

curricula. Most evidently are the ever present global environmental concerns. Representatives in this field also feel the need to have such content taught at a lower-level so as to help bring up an environment-conscious individual (Lestch, 2015). What to include and what to leave out then becomes a significant hurdle in itself for the key stakeholders to overcome, as it is rather challenging to know what selection criteria to use, according to Lestch (2015).

Factors that Limit the Use of School Curricula

Some positive steps that could be taken in a bid to address this concern are such as that which was proposed by Galloway's office, following the Missouri state audit of the five districts (Doran, 2016). These are assigning a district security administrator who will regularly assess the allocation of digital account privileges, to train staff on cyber security issues and having in place an improved vendor monitoring system. Galloway's office also suggests having k-12 officials regularly change their passwords and training teachers on best practices for managing student data (Doran, 2016). As they constantly engage in such simple safety procedures, they will better appreciate their need and will be more willing ambassadors in having such information included in the k-12 curriculum.

Another initiative would be running cyber camps in these k-12 schools, with each customized for the different age groups and classes. It is an idea borrowed from an initiative that proved successful in Charlottesville High School, Virginia. The cyber-camp was done to expose students to computer science and cyber security. The camp was sponsored by a Virginia Department of Education Grant, a move which again proves the critical role the state education department has to play in developing a cyber-security conscious population (NICERC, 2015). The desired outcome of such regular cyber-camps is not only to get students interested in cyber-security & the related careers but also to help school management realize the need of having such

content included in the school curriculum, especially after observing an increased interest in the subject by more and more students. Further borrowing from this initiative, the program can be structured in the curriculum to include robotics, cyber-ethics and how the Internet and cyber-security fit into society. As it stands, the Federal Department of Homeland Security has projected demand for 2.5 million additional cyber security positions over the next five-year period (NICERC, 2015). What better way to help close this gap than to raise cyber security awareness at the earliest possible levels?

To overcome the challenge of having few educators who appreciate the value of cyber-security, schools should seek to adopt federal government programs that aim at educating teachers on subjects, such as the Integrated Cyber-Security Education Communities (ICEC) Program. It provides teachers with the training and tools needed to integrate cyber security skills in the classroom. It is also designed to encourage interest in the cyber security field and increase awareness of cyber security careers and academic pathways among high school students (NICCS, 2016). With more and more educators going through such programs, they will soon be the advocates for such cyber-security training to be implemented in the school curriculum.

Further efforts are required to develop national and state content standards for computer science (Computer Science Teachers Association, 2003). As it already stands, cyber-security is a sub-discipline of computer science. School curriculum standards then help define the knowledge and skills needed to be acquired by each student. For this effort to be successful, school curricula must be aligned with these national and state-level content standards. The curriculum process development will further include the involvement of university faculty and professional organizations, such as ACM & ISTE (Computer Science Teachers Association, 2003). More so, the National Council for Accreditation of Teacher Education (NCATE) also took steps towards

addressing the situation by having define accreditation standards for secondary computer science education programs (Computer Science Teachers Association, 2003). This endorsement program is equated to providing future teachers with a minor in Computer Science. However, NCATE states to undertake this course one is required to have a foundation in educational technology because it is a positive step by existing authoritative bodies towards closing the existing gap in cyber security, and by extension, computer science trainers at k-12 level schools (Computer Science Teachers Association, 2003).

By teaching safety basics in school districts, as highlighted by an article by ‘Plante Moran’ dubbed *Avoiding a data breach: Cyber-security at K-12 institutions*, “Education is the first line of defense against a cyber-attack” (Plante Moran, 2015). The article suggests not only including teachers and students in cyber-security training but also parents. The article further suggests such training should cover the basics of choosing and changing passwords to appropriate use of devices connected to the school’s network (2015). Plante Mornan also believes this will prove helpful as it will target students who are more often responsible for the security breaches at schools as it will emphasize both ethical issues and the serious consequences of illegal hacking (2015). With the continued implementation of such a training program and the realization of its benefits, key stakeholders will need little convincing to include cyber-security in the school curriculum (Plante Moran, 2015).

Though advocating for the inclusion of Computer Science in k-12 school curriculum, the Computer Science Teachers Association in their report, *A Model Curriculum for K-12 Computer Science: Final Report of the ACM k-12 Taskforce Curriculum Committee*, acknowledge that, “...persons in leadership positions must acknowledge the importance of computer science education for the future of our society. States and accrediting organizations should make this a

factor in overall school accreditation” (Computer Science Teachers Association, 2003). The report also acknowledges that some countries have begun making efforts towards this. The Computer Science Teachers Association concluded this report by proposing a Model Curriculum that could be adopted for k-12 Computer Science (Computer Science Teachers Association, 2003). Whereas the model is fairly representative of all Computer Science subject areas, it fails to cover the most urgent concern of cyber-security. However, given that the report was prepared in 2003, it is most likely that improvements have been made upon it to include cyber-security. The report suggests establishing suitable standards for teacher certification. It is the development of one such model curriculum by authoritative bodies in the field of cyber-security that will help all stakeholders understand the need of having this subject introduced in the curriculum (Computer Science Teachers Association, 2003).

The Computer Science Teachers Association report also suggests Professional organizations can also get involved in helping push this motion forward, such as ACM, the IEEE Computer Society, ISTE, institutions of higher education, and national and local teacher organizations (2003). Such organizations are better positioned, being more authoritative and better funded to advocate for the inclusion of cyber-security in school curricula (Computer Science Teachers Association, 2003).

The National Initiative for Cyber-Security Education, in their ‘National Cyber-Security Workforce Framework,’ feels another positive initiative would be making students aware of the existing careers within the sub-discipline of cyber security that classifies cyber security into seven high-level groups, and further, lists some these specialty areas within each group (Raytheon in conjunction with the National Cyber Security Alliance, 2014). Following this framework, teachers and career mentors can suggest these specialty areas to students throughout

their school life as possible career options, in addition to the other more familiar career choices (Raytheon in conjunction with the National Cyber Security Alliance, 2014).

Another opportunity lies in the deliberate realization by school management and state education departments of the increased interest in cyber security concerns by the younger generation. The interest already exists amongst the teenagers, which with little effort, can easily trickle down to k-12 level students. It is an already existing opportunity that only needs to be harnessed through proper strategies; one of which would be increasing the k-12 level students' cyber-security knowledge through their school curricula (Raytheon in conjunction with the National Cyber Security Alliance, 2014).

In the *Journal of Advances in Information Technology*, it suggests a personal initiative have a review of the prevailing statistics of the number of k-12 students who currently participate in cyber-attacks of various forms, whether knowingly or not, may serve as a wake-up call to the teachers, school management and school district administration staff to advocate for the inclusion of cyber-security training in the curriculum (Aloul, 2012). The journal states this can be done with the hope of helping the students involved in these notorious activities understand the ethical and even legal dimensions that come into play when one engages in cyber-attacks (Aloul, 2012). According to Computer Science Teachers Association, to further feed this flame would be a review by the concerned stakeholders of the daily cyber attack reports that are present in the news channels, online and even through social media (2003). As it stands, cyber threats and cyber attacks have now become the newest weapon of mass destruction. Countries are going to great lengths to secure their networks and data as they realize that such could be used to hold an entire nation hostage, especially with the advent of the concept of 'The Internet of Things' (Aloul, 2012). The risk presented is that all devices will be interconnected and can then be

controlled from a central point. It is frightening even to consider the amount of damage that could ensue. Being such a national concern, it only follows that the best way to tackle such an issue is from the ground up, and this will in every way include cyber-security training in schools at the lowest level possible (Aloul, 2012).

Discussion of the Findings

The purpose of this research was to examine the need for cyber security education implemented in classes to children in the k-12 school curriculum. What are the curricular approaches or school-based strategies tried in teaching cyber security, safety, and ethical conduct in k-12? What are some of the impediments to the formation, adaptation and implementation of a curriculum that addresses cyber security? How can the factors that limit the use of school curricula in combating cyber security be surmounted?

As emphasized by Rowe, Lunt, and Ekstrom (2011), our world has now moved into the digital realm where computers and the Internet have become an integral part of everyday life. In the past, computers were used for the purpose of entertainment and played other minor roles that would not have put its users at risk. However, as technology advanced, high-tech machines are being used for a lot more than just play. Along with these changes are equally outrageous threats and an unprecedented rise in cyber crime rates. As pointed out by Aloul (2012), the increased usage came with risks that potential users had to manage. The Internet has now become a hub where a variety of activities, such as socializing and making purchases, take place. They have become a central part of people's lives. As a result, it is prudent to address some of the risks users expose themselves to.

The virtual world epitomizes an environment where there may be a greater license to participate in unjustified behavior because of the anonymity and the ability to mask one's

identity. Students need to be cognizant and understand that there is no such thing as perfect security. Prohibited cyber attacks come through the establishment of protection strategies and education. Cyber security is one of the key issues that computer users need to know and one of the most critical economic and national security challenges we encounter as a nation.

Enlightening the public on how to remain safe in the cyber world is a key necessity. In the past, the issue had only affected governments and large corporations. However, more than 3 billion people are now using the computer more frequently and the Internet for more tasks (Davidson, 2015). One reason Internet access has surpassed over the past 15 years is the rising affordability and availability (Davidson, 2015). As cited in Lestch, the executive director of the National Cyber Security Alliance, Michael Kaiser stated, “Using technology is one of the three ‘Rs’ of the 21st century.” He further proclaimed, “If you do not graduate from high school knowing how to use technology, it is going to be a hindrance in the same way if you do not know how to read” (2015). The three R’s are referencing the traditional subjects of reading, writing, and arithmetic.

Technology has had a tremendous impact on the education sector. The increased incorporation of technology into the world systems has brought with it a fair share of merits and demerits of the society as a whole. In the education community the merits have included; enhanced access to information through internet searches. Technology has made it easier to access academic information through blogs, websites, online journals, online tutorials, and online libraries. It has increased children’s participation in learning since they can take initiatives to acquire new things or seek clarity on difficult subject matters. The internet especially simulates learners as it offers exciting ways to learn which is what childhood and young people like to explore. Social media has also made it possible to keep up to date with general information and interact with people across borders. Most children and young people tend to spend most of their

time online and share personal information and updates of their day to day activities especially on social media unaware of the risk they might be exposing themselves to. Consequently, children and young people have been victimized by criminals in cyberspace because most of them are vulnerable due to lack of knowledge of cyber crimes and cyber security. They are, therefore, not in a position to identify impending threats of attack or act when the attack happens. In some instances, some are not even aware that they are victims of a cyber attack as in the cases of cyber stalking, cyber bullying, and predators. Some young people have also been engaged in the attacks as perpetrators unconsciously because they lack awareness of ethical standards in the virtual space.

Cyber-crime and transnational organized crime have been known to thrive in the virtual space. It is growing concern over the same that has raised awareness of cyber security issues and consequently measures and policies being adopted at different levels by various sectors within the state. It has also led to the need to incorporate cyber security into the curriculum for k-12 schools since young people today are exposed to technology and internet use at a very early age. It means that they are equally vulnerable to the risks and attacks within the virtual space at a very young age. It hence goes without saying that there is a need to safeguard children and young people and nurture them into responsible consumers of technology by equipping them with the adequate knowledge and skills on cyber security, cyber ethics, and cyber safety. Teaching cyber security in k-12 schools is deemed necessary because traditionally schools have always had the responsibility of socializing and training the young people. Schools have also adopted technology in learning to provide students with guidelines and safety precautions for the use of technology. Exposing the youth to cyber security issues during their formative years makes it in

an integral part of their lives. The school setting being a formal setting always gives weight to the issue of cyber security to young people.

In 2008, a survey was conducted to explore the nature of Cyberethics, Cybersafety, and Cybersecurity (C3) educational awareness policies, initiatives, curriculum, and practices that are currently taking place in the U.S. public and private k-12 educational settings (Pruitt-Mentle, 2008). This research found the state C3 Education incomplete. According to the Pruitt-Mentle research study, Cyberethics, Cybersafety, and Cybersecurity are limited, and the standards on the content were limited. It is because some C3 information was passed on to children through school policy papers-(Acceptable Use policies); most of which are centered on a particular's school's rules and regulations regarding use of technical tools within the school. These policy papers limited opportunity for threats by restricting access to internet connectivity and computer usage without covering much of C3 content. Educators also did not feel comfortable discussing the topics although the responsibility had been left to them by their respective states and education authorities. It meant that children and young people had the responsibility of comprehending the C3 content on their own from the policy papers. It is evidence of the existing gap between policies and the implementation of the same. Some schools tried bridging this gap by having external presenters, like people from police departments, attend events where they would seek to explain issues of cyber ethics, cyber safety, and cyber security. These efforts are, however, limited in the sense that the talks are once while in a while occasion and therefore, less efficient means of promoting the culture of responsible use of cyberspace among children and young people. People also felt that addressing the content of C3 and solving these cyber problems were the educators' responsibility; yet, in theory, C3 content is not mandated (Pruitt-Mentle, 2008). C3 should be the responsibility of all, and addressing the dearth of knowledge

and developing a sense of responsibility can start with parents and educators. Just as a parent teaches their child right from wrong, parents also should take the necessary steps of teaching their child how to be ethical when using a computer. Educators should come into play by providing more in-depth knowledge about the subject.

The challenge has been that the curriculum of topics related to C3 education such as computer science focuses more on skills than ethical standards of technology. Also, the educators handling technical subjects focus on areas that are tested in state examinations such as knowledge of new technologies and hands-on use of the same, at the expense of educating students on C3 contents. It is possible because the educators also received minimal training on C3 education during their training years as classroom teachers. The curriculum has been such that people who are not pursuing Information Technology or Computer Technology courses receive basic training on computer packages. In some schools and institutions of higher learning, even these basic computer classes are not offered unless the students are enrolled in computer specific courses. Even for educators who underwent some training on the cyber security are faced with the challenge of changing security threats and coping with the changing threats. Data from the survey of educators also indicated that 67% of respondents did not know how to update anti-virus, spyware, and anti-spam filters, and 52% did not know how to install operating system patches. Over 25% were not at all prepared to discuss basic Cyber safety issues, and amazingly, 75% of educators felt uncomfortable discussing topics that have had significant public attention, like cyberbullying (Pruitt-Mentle, 2008). This kind of feedback from those entrusted with the task of conducting C3 education raises a concern of the success of C3 education in k-12 schools. If those expected to equip the children and young people are quite unequipped themselves, one is then left to wonder how C3 content is carried out in the school systems. It is a reflection of a

disconnect between the policy makers and those expected to implement the same. Although C3 education may be incorporated in educational policy as part of the curriculum for k-12 schools, if educators are not equipped with skills to handle the topics, then the policies will hardly be translated into action. The school administrators as can be perceived from this reports, do not portray a will to implement C3 education effectively by advocating for professional development training for educators within their schools. District officials are also laid back on this issue because if monitoring and evaluation would be carried out, then the need for in-service training would have surfaced and measures to address the same would have been put in place.

According to an article in Journal of Digital Learning in Teacher Education written by Portia Pusey and William A. Sadera, two federal laws, in the past two years were approved that modified k-12 education (2011). The two federal laws place less significance on standardized testing as compared to the former laws. Under these laws, the states and local authorities are also responsible for schools that are considered to be underperforming. They are mandated with upgrading the five least performing schools in their districts. The law reduces strict federal control over schools, giving states control over schools within their territorial boundaries. It allows for flexibility since the states can substitute state and local tests with other means for testing achievement. School administrators and educators can also put in their contributions in the education system through contributing to policy reforms based on students need they have been able to identify in the course of their duty. This flexibility allows for smooth incorporation of cyber security into the k-12 education system and schools with the help of technology coordinators. As earlier stated educators tended to focus on subject areas that would count in state test scores at the expense of others that were viewed as less important since they were not reflected in state test scores. The room for considering access to resources when assessing

children and substituting local tests encourages educators to give equal weight to all courses. The content of technology related courses can also be expanded and adjusted to include C3 education on a comprehensive basis. Under this new policy, funding is also made flexible for k-12 district schools. The district officials can appropriate federal resources based on their local needs. They can, therefore, prioritize funding C3 education process since the lack of funding to implement the program has been one of the challenges cited by the district officials. Restoring local control allows districts that have realized the need to implement cyber security education, carry on with the program by acquiring necessary input and training on the same for their educators who will pass it on to children and young people. It is necessary since C3 education may not be welcomed with the same enthusiasm in all states, districts, and even schools. Some educators feel that it is not entirely their duty to carry out C3 education except on a few ethical issues that affected learning directly like plagiarism and referencing. The rationale is that the Children's Internet Protection Act (CIPA) forces schools to have a clear Internet safety policy and so children are more at risk at home and other places outside the school. Educators with this perception argued that teaching young people C3 topics was the responsibility of parents.

Recommendations

Based on the findings that have already been discussed, this study presents some recommendations which will be discussed separately but overlap and are consistent in contributing to an informed policy framework on teaching cyber security in k-12 schools. The recommendations not only capture cyber ethics, cyber safety, and cyber security, for children in k-12 schools but cyber security for the school administrators, educators and the education community as a whole.

There is a need to restructure the curriculum in k-12 schools so that cyber security is covered comprehensively as a subject. Among the findings discussed, there were two federal laws adopted by the government of the United States that provided room for local authorities to adjust their education programs accordingly. However, these laws and requirements are broad and unclear in their strategy and suggestions (Pusey & Sadera, 2011, p. 82). Even at the state and district level, there ought to be clear guideline and systems that have been put in place to ensure that C3 education is part of the curriculum. At the local level, monitoring by k-12 district officials should be carried out to ensure implementation of C3 education and to see to it that educators and school administrators adhere to core standards on matters of cyber security. For instance, some schools can choose only to deal with one aspect of the C3 content like cyber ethics and ignore the other aspects of cyber security and cyber safety. It would give the impression that C3 education is carried out in these schools, yet the coverage is incomplete and touches only on a few issues on the surface. Numerous curriculum resources are available within and outside the federal government. The Integrated Cybersecurity Education Communities (ICEC) is an example of a federally sponsored program while others that are not state sponsored include StaySafeOnline, IKeepSafe, Association for Computing Machinery, Cyberwatch, Security Injections, Stem Robotics, and Software Assurance Curriculum, just to mention a few. These curriculum providers endeavor to develop curriculum recommendation for k-12 schools and colleges and provide teachers with training and tools they need to stay updated in the phase of rapidly changing computer technology. Such resources need standardization before being adopted by k-12 schools. It is because these providers are entrepreneurs in the market competing for clients. Also, the information offered by various providers on one subject issue is contradictory. Rowe, Lunt, and Ekstrom recommend that where possible, k-12 schools introduce

an advanced model of cyber security based on prepare, defend and act model (2011). Along with this, schools also need to expand their acceptable use policies in a bid to facilitate awareness on cyber security.

Educators expressed feelings of unpreparedness to tackle C3 education in k-12 schools. The majority of educators confessed that they had a limited awareness about most C3 topics (Pruitt-Mentle, 2008). This lack of understanding prevented them from sharing information with students in either formal lessons or informal settings. It is because educator technology training has been focused toward integration techniques, developing skills and providing students with opportunities to use technology. This training, however, has been lacking in C3 content, and this explains the state of unpreparedness among educators. According to the National C3 Baseline Survey results, 90% of educators have received less than six hours of professional development on C3 topics in the last twelve months. The results also indicated that 67% of educators are willing to learn more about C3 topics but lacked such professional opportunities (Pruitt-Mentle, 2008). It confirms the need to for professional development, preferably in-service training, for both technology coordinators and educators. It complemented with hands-on training opportunities for educators and increased C3 awareness opportunities for youth throughout the k-12 experience would provide the comprehensive effort needed to deal with threats in the virtual space. Such training needs to be conducted on a regular basis as refresher training for educators to cope with the changes in technology and cyber threats and cyber attacks.

Digital updating of C3 content and policies is necessary. It is because, with the change in technology: cyber threats, crimes and attacks also change. The more complex technology develops, the more complex the challenges that come with it. There is thus need to cope with these changes to minimize the demerits of technology. C3 content and education policies thus

need to be periodically reviewed and updated. It can be very costly if the updates have to be done using hard copy materials, such as printed forms. It is, therefore, more cost effective to update digital C3 content. The state, education ministry, and other relevant stakeholders also need to review periodically policies that affect the education sector, such as funding for C3 education. Failure to review policies is a drawback to the education sector and implementation of C3 education as well. Such was the case when the “No child left behind” policy expired in 2007, but was only replaced seven years later (Mary Troyan, 2015). Periodic reviews of C3 content makes it relevant to the challenges presented by modernity and advancements in technology. The result would be young people who are thoroughly equipped with the day to day threats posed by criminals in the virtual space. It would also imply regular professional development training for educators. It has been discussed in depth in the previous recommendation.

C3 education should not be viewed as a sole responsibility of educators. The society other than the education community, have a role to play in promoting cyber ethics and safeguarding children and young people online. If the responsible use of the internet is to be embraced as a culture among children and adolescents, then it has to be part of their lives at home, in school and other social networks because socialization does not take place in school only. Both the educators and parents ought to stop shifting the responsibility to the other party but collectively take up the duty of equipping the children and young people with Cyber security knowledge. Educators may, however, be in a better in a better position to handle C3 topics comprehensively. They are equipped with instructions and learning materials on C3 topics, unlike parents who may have limited access to such resources. Some parents are also computer illiterate while some have limited knowledge of C3 topics. Nevertheless, parents need to show concern and a keen interest in their children’s social lives, including their online activities.

Services from experts in the field of cyber security can also be tapped to combine real-world experiences with learning for young people in seminars, recreation programs, and etc.

Furthermore, cyber security is a trans-national security concern and requires international cooperation to deal effectively with the issue. Insights from international organizations that deal with cyber crimes, cyber security and monitoring of the digital space can also be used to build robust computer networks in k-12 schools and develop content for C3 education in k-12 schools.

The identity ecosystem of April 2011 also aimed at curbing cyber crime by putting in place standards to authenticate identities of internet users, as well as their devices (Finklea & Theohary, 2012). This measure is inclusive of policies and security guidelines aimed at protecting the individual, organization and their assets within the cyberspace. k-12 schools have been victims of cyber-crimes in the form of students hacking into accounts to change their grades. An incident occurred where “about 15,000 students at Sachem School District in Long Island, New York, had personal data, including school ID numbers and the names of those receiving free or reduced lunches, posted to an online forum (Newsday, 2013). Again “... an experienced external hacker seized the computer systems at Swedesboro-Woolwich School District and held them for ransom – making it incredibly difficult for kids at four primary schools to do their web-based statewide examinations as scheduled” (Niekerk & Solms, 2013). The hacker gained access to the network through a vendor who provided maintenance work the network. The third-party vendor was said to have a weak password to the network. Schools need to be deliberate in strengthening and protecting their critical data such as those of teachers and students. Data containing personal information and social security numbers should be protected by building robust networks. School administrators also need to enquire on the credibility of third-party vendors before they are allowed access to the school’s network. Implementation of

the identity ecosystem by k-12 schools would make it difficult for criminals to gain access to a school's network and interfere with its online transactions. It would also facilitate recovery of data that would ensure criminals are traced and prosecuted. This system also prevents cyber espionage.

Most people have embraced the rapid development in computer and telecommunication technologies. However, design flaws in information systems and reckless use of the same have made communication technology vulnerable (Kizza, 2005). Lunt argues that with the ever increasing cyber threats, there is need to educate students on the concepts and skills of cyber security. This responsibility he argues is a key responsibility of academic institutions in the United States (Rowe, Lunt, and Ekstrom, 2011). Educating children and young people on cyber security makes the more alert and careful when using technological devices. Advancement in technologies should not make its users subject to misuse and abuse. The cyber security approaches have not advanced proportionally with the advancements in digital services and technologies. An ideal situation is one where the manner and rate at which exploits are done in technological development is supposed to be the same rate that strides are made to secure the consumers of technology. The school is a very powerful socializing agent, and so if children undergo training on cyber ethics and cyber security as part of the normal learning process, then they will grow into the culture of safe and responsible use of the cyberspace.

Cyber security is focused on the safety computer programs, data, and networks from unauthorized access and destruction (Kizza, 2005). Enlightening the public on how to remain safe in the cyber world is a key necessity because, with an increase in mobile users, digital networks and applications, the chances for exploitation also increase. In the past, the issue had only affected governments and large corporations because they collected and stored much

personal information on computer networks. Access to such information is a huge threat to an organization's security; digital spying can be used to launch attacks on a state. For instance, China has been known to attacking other countries online and is targeting electrical dominance over its rival states by 2050 (Andreasson, 2011). Currently, this threat and attacks has moved beyond organizations to individuals inclusive of children and young people. According to Kizza, some threats within the cyberspace are as a result of loopholes within the software and hardware of a computer system. Most of the people using the digital devices are not security experts and thus, not able to identify the loopholes and even when they do, they do not know how to respond or where to report (2005).

Children and young people tend to be frequent users of computer networks in school and social media for entertainment. Most of them believe that because their interaction with computer networks is limited to these spheres, they are safe. It is a false belief because most computer networks and social media sites require authentication details and sometimes we have to register our details on such sites (Easttom, 2013). This alone is enough to make a threat, especially when one uses personal information such as real name, home address, or work address on those sites. Cyber security awareness will help individuals reduce vulnerabilities and minimize exposure to potential cyber attacks. Most people do not prioritize cyber security issues until they become victims of cyber-attacks. It can be blamed on socialization and lack of training on the same both at home and in schools in the formative years of most of these people. Any data that contains personal information such as one's social security number must be protected because access to such information can lead to significant damage. Increased online security would consequently mean increased complexity (Doran, 2016). Most people naturally are uncomfortable with complex procedures when there are much simpler alternatives. It has been

identified as a cause for vulnerability even at individual levels because most people do not comply with the security policies on most sites on the internet.

Children and young people are increasingly becoming technology consumers. They are equally exposed to cyberspace attacks just as much as adults. It, in turn, leads to the need to address the online security of young people. Failure to attend to the security concerns has an impact on the children's and young people's psychological and social development. Continuous exposure to the negative influences of technology can lead to detrimental behavior. For instance, a young person on social media can receive pornographic images or videos from a sextortionist and find it repelling at first. If the victim is silent over the issue and does not know how to stop it either, the result may be an addiction to pornography. It may occur when the young person continues receiving and viewing the material. The need for cyber security education in k-12 schools cannot be over emphasized. Since these are the formative years of a child and young people, it is the lowest level that students can be able to appreciate the weight of the matter and develop an interest in promoting cyber security both in their personal lives and to the general public.

Integration of cyber security education into the k-12 school's curricula is one of the effective ways to implement education on C3 content. Some curriculum guidelines have suggested that C3 content is tailored to be audience specific. Their content should be categorized depending on the grade of students targeted. It will enable them to relate to the content. Peer education is also a great tool of empowerment since it challenges the young people to be more informed on the subject of cyber security. Besides that, peer influence is a good way to socialize young people into responsible use of cyberspace. It is because, at this stage of development, most young people in the adolescent and teen stage always seek to fit in peer groups. NetSmartz takes

advantage of this sociological behavior to influence young people into positive awareness of cyber security. Adopting security in the curriculum is, however, a challenge because it would mean more workload for the educator. Regarding the preparation, they would need to deliver the contents of cyber security education. According to the Pruitt-Mentle report, most educators admitted to being ill equipped to conduct cyber security education (Pruitt-Mentle, 2008). On one hand, among the parents and guardians, this measure may be gladly received as their children would be the beneficiaries of such an enlightenment. On the other hand, integration of cyber security education into the curriculum would mean compulsory development training for the educators who may be unwilling to undertake the training. For C3 education to remain relevant, there will be the need to update frequently the content to address emerging threats and trends. The flexibility of the k-12 curriculum may not be as rapid as the changes in technological developments. Frequent change of the curriculum will also make it unstable and ineffective. It is because sometimes a long period elapses between the conception and delivery of a new curriculum. By the time it is being implemented, it is almost becoming irrelevant due to social transformation, changes in the world market, and globalization.

The benefits of cyber security education in k-12 schools outweigh the challenges. Early exposure to cyber security content can motivate young people to consider it as a career choice. It will also make it easy for young people who get to college to easily grasp cyber crime and cyber security concepts. It will be unlike the pressure that young people face when first exposed to the subject at the college level. In fact, for a long time, due to this pressure those students face at college and campus level, they have propagated the notion that computer science, information technology, cyber crime, cyber security, and other related courses are difficult to conceptualize and are reserved for 'geniuses.' It explains the limited numbers of information technology

specialists and cyber security specialists. By the time most students are in the senior year of high school, they have settled in the careers they want to pursue and consciously working towards it, regarding academic scores, applying for scholarships, and college. Early exposure to this discipline will also increase the number of cyber security specialists in the United States. It has been an issue of concern because even in such a technologically equipped and well-funded state, the number of cyber security specialists is limited (Rowe, Lunt, and Ekstrom, 2011). Currently, with the rapid technological advancements students are taking on more science oriented and technical courses.

I would recommend not only including teachers and students in cyber-security training but also parents. The teachers may be well equipped and educate students on online safety measures and ethical issues, but if the same standards are not observed at home, then the home may act as loopholes where the child is exposed to cyber-attacks or is free to violate cyber ethics. It will water down what the educators are trying to nurture in school. The inclusion of parents in the training of cyber security will also help to bridge the generational gap between the parents and the children. Some parents are not techno-savvy and therefore, not able though willing to provide guidelines on safe use of digital devices. Once parents undergo the training, they can effectively protect themselves and their children from cyberspace criminals. Also, the parents and educators can learn from these trainings on how to treat reports of cyber-attacks from their children and students so that they will not over react or under react to such reports.

Future Research

New Research Question 1

Reading from Pruitt Mentle's report on the survey conducted in 2008 to explore the C3 educational awareness policies, initiatives, curriculum, and practices currently taking place in the U.S in private and k-12 schools, an interesting debate almost ensued on whose responsibility

was it to teach children and young people on C3 topics. Most respondents in the survey indicated that it was the role of educators to carry out C3 education. The majority of the educators felt that it was the role of parents to conduct C3 education to their children. They further admitted not knowing how information on C3 contents was passed on to the children within their schools (Pruitt Mentle, 2008). The aim of that particular survey was to find out how C3 courses were being addressed through the school systems and were therefore largely focused on the role of educators in C3 education. However, it would be substantial in that future research studies delve into the role of parents in cyber security. It is necessary because schools are required by The Children's Internet Protection Act (CIPA) to have a clear Internet safety policy. The policy protects students from contact with offensive content through the use of Internet filters. So children are more at risk of cyber-attacks at their when using computers at their homes or other unrestricted environments. Also, parents are the first educators of children before they step into k-12 schools. Children also tend to run to their parents when things are not working out, and the same should apply when children face threats in cyberspace. It means that parents have a role to play in identifying the child's cyber threats, in protecting family computers, mobile devices and talking about these issues with their children. Some parents based on their level of knowledge tend to overreact, while others rarely react when children report such incidences to them. Parent's response to reports of cyber-attacks by their children can deter or encourage children to report recurring incidents. For example, when a parent responds by taking away a child's internet privileges, such a child may shy away from sharing such incidents with the parent in future. Some parents dismiss children's claims or even blame the kids for being victimized. The child, therefore, suffers exposure to cyber threats in silence. A child is also likely to be the cyber bully. The victims and parents need to know how to tell the difference. Research has acknowledged the

significance of ongoing discussions between parents, guardians, and caregivers and their children about online activities (Berson, 2002). A study on the same can help shade some light on the gray areas.

New Research Question 2

Another recommended future research question is how to curb cyber crime in banks. Online theft in banks is an increasing predicament that needs to be looked into exhaustively. The associated criminals hack into the bank systems through the employees' computers and then spread the virus to all networks within the bank system taking control of all the bank's operations. They then take the time watching the moves and daily activities of the employees until they find a chance of lifting huge amounts of money from the victim banks. The USA TODAY magazine dated February 16, 2015, states a scenario where a security firm Kaspersky Lab operating in Moscow came up with a report showing how criminals managed to go home with billions of money from 100 banks across 30 countries. They managed to siphon the money by installing malware that enabled them to take control of all the internal operations of the banks. It is, therefore, prudent enough to do research on how to curb bank cyber crimes and if possible identify such criminals and bring them to justice.

New Research Question 3

The other key recommended future research question is the global impact of Cyber Security, Cyber Ethics, Cyber Safety among the k-12 Schools. As discussed in this thesis, the implementation of C3 education has not been widely effective. The researcher has recommended some ways to enforce them in the k-12 schools. However, what remains unclear is the impact of such initiative globally among the k-12 schools and the society as a whole once undertaken. The researcher here is positive about the outcome of such initiative but not

optimistic of the results. Once 3Cs have been introduced and enforced among k-12 schools, the cyber criminals as well do their best to adjust to the system. In future, some of the criminals will be products of k-12. It is to carry out research on the global impacts that are implementing the C3 education has globally, within our societies.

References

- Andreasson, K. J. (2011). *Cybersecurity: Public sector threats and responses*. CRC Press.
- Aloul, F. A. (2012, August). The need for effective information security awareness. *Journal of Advances in Information Technology*, 3(3), 176-183. Retrieved from <https://www.semanticscholar.org/paper/The-Need-for-Effective-Information-Security-Aloul/88ea44e00882c347dcad6710328744eb684b47e9/pdf>
- Australian Communications and Media Authority. (2011). *An overview of international cybersecurity awareness raising and educational initiatives: Research report commissioned by the Australian Communications and Media Authority*. Melbourne: Australian Communications and Media Authority.
- Caputo, D.D., & Pfleeger, S.L. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4), 597-611. Retrieved from <https://www.semanticscholar.org/paper/Leveraging-behavioral-science-to-mitigate-cyber-Pfleeger-Caputo/e755aa8baf01ef655ef7b1472ceba505b7c45b91/pdf>
- Computer Science Teachers Association. (2003). *A Model Curriculum for K-12 Computer Science: Final Report of the ACM k-12 Taskforce Curriculum Committee*. New York: Association for Computing Machinery, Inc (ACM).
- Davidson, J. (2015, May 26). 3.2 Billion people now using Internet worldwide. Retrieved from <http://time.com/money/3896219/internet-users-worldwide/>
- Doran, L. (2016, April 27). *State k-12 Cybersecurity Audit Finds Missouri District Unprepared*. Retrieved from Education Week: www.edweek.org
- Easttom II, W. C. (2013). *Network Defense and Countermeasures: Principles and Practices*. Pearson IT Certification.

- Ekstrom, J.J., Lunt, B.M., & Rowe, D.C.. (2011, October). The role of cyber-security in information technology education. *SIGITE*. Retrieved from <http://sigite2011.sigite.org/wp-content/uploads/2011/10/session07-paper03.pdf>
- Kizza, J. M. (2005). Computer network security. Springer Science & Business Media.
- Lestch, C. (2015, July 19). *Cyber-security in k-12 education: Schools face increased risk of cyber attacks*. Retrieved from fedscoop.com: www.fedscoop.com
- Pruitt-Mentle, D. (2008, October). 2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study. Retrieved from http://www.edtechpolicy.org/cyberk12/Documents/C3Awareness/NationalC3BaselineSurvey_Extract_sept_2010.pdf
- Lestch, C. (2015, July 21). Reading, writing — and cybersecurity? Digital safety programs sprout up in schools. Retrieved from <http://fedscoop.com/cybersecurity-is-being-taught-with-reading-writing-and-arithmetic-in-schools>
- National Cyber Security Alliance, McAfee, and CyberSmart! Education Team Up to Bring Cybersecurity Learning Resources to K-12 Classrooms. (2011, October 24). *Bioterrorism Week*, p. 16. Retrieved from http://go.galegroup.com/ps/i.do?id=GALE%7CA270473629&v=2.1&u=nysl_ce_uticacol&it=r&p=AONE&sw=w&asid=3c3790931e0c7ff197080985bde5b45c
- National Initiative for Cybersecurity Careers and Studies (NICCS). (n.d.). Stop.Think.Connect.™ Campaign. Retrieved from <https://niccs.us-cert.gov/awareness/stop-think-connect%E2%84%A2-campaign>
- NetSmartz Workshop. (n.d.). Educators. Retrieved from <http://www.netsmartz.org/Educators>

- New York Internet Crimes Against Children Task Force. (2012). Internet safety. Retrieved from <http://www.nysicac.org/index.php/links/internet-safety.html>
- NICCS. (2016, February 17). *Curriculum Resources: Teaching Tools for Educators*. Retrieved from National Initiative for Cyber-security Careers and Studies (NICCS): <https://niccs.us-cert.gov>
- NICERC. (2015). *Cybercamp introduces CHS students to cybersecurity careers*. Retrieved from NICERC: An Academic Division of the Cyber Innovation Center: www.nicerc.org
- Niekerk, J., Reid, R., & Thomson, K. (2013). Cyber Safety for School Children - A Case Study in the Nelson Mandela Metropolis. *ifip11-8*. Retrieved from <http://dl.ifip.org/db/conf/ifip11-8/ifip11-8-2013/NiekerkTR13.pdf>
- Niekerk, J., & Solms, R.V. (2013, November 11). From information security to cyber security. *Computers & Security*, 38, 97-102. Retrieved from <https://www.semanticscholar.org/paper/From-information-security-to-cyber-security-Solms-Niekerk/fe08518ae297cef31d99092e97e8d323a378f81f/pdf>
- Plante Moran. (2015, December 03). *Avoiding a data breach: Cybersecurity at K-12 institutions*. Retrieved from plante moran: www.plantemoran.com
- Pusey, P., & Sadera, W. A. (2011). Journal of Digital Learning in Teacher Education. *Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference*, 28(2), 82-88. Retrieved from <http://files.eric.ed.gov/fulltext/EJ960154.pdf>
- Raytheon in conjunction with the National Cyber Security Alliance. (2014, October 13). *Millennials and Cybersecurity Careers*. Retrieved from k-12 Cyber Security Education Think Tank: www.edtechpolicy.org

U.S. Schools not preparing kids for digital age. (Cover story). (2011). *Computer Security Update*, 12(6), 1-5.