

5-14-2019

# K-12 Cybersecurity Program Evaluation and Its Application

Tabitha Domeij
*Bridgewater State University*

# K-12 Cybersecurity Program Evaluation and Its Application

Tabitha Domeij

Submitted in Partial Completion of the
Requirements for Commonwealth Honors in Criminal Justice

Bridgewater State University

May 14, 2019

Dr. Kyung-shick Choi, Thesis Advisor
Dr. Feodor Gostjev, Committee Member
Prof. Stephen Simms, Committee Member

## ABSTRACT

As the use of the Internet and computers continues to increase, so does the prevalence of cybercrime. However, there is currently no global standard education curriculum guideline in place to prevent cybercrime or cybercrime victimization. The purpose of this study is to examine programs designed for students in grades K-12 that have already been implemented in communities across the country in order to determine the amount of information taught and to identify a global standard preventative program for all educational institutions. This project will be an exploratory study in which existing K-12 curriculum programs are reviewed qualitatively using a content analysis method based upon the theoretical framework of Choi's Cyber-Routine Activities Theory (Cyber RAT) (Choi, 2008). The expected outcome of this research is to identify and create standards for an ideal cybersecurity educational program for students in grades K-12. This research is timely and imperative in the field of criminal justice because crimes are becoming increasingly prevalent in the cyber-world with very limited means available to control or prevent them. Findings in this study suggest that most programs teach students a sufficient amount of topics relating to computer hygiene, computer ethics, and technological skills. However, further research must be conducted to determine the quality of these programs in adequately informing students about topics involving cybersecurity and cybercrime.

## INTRODUCTION

Despite a constant increase in technology use by K-12 students, there is currently no standard educational curriculum that thoroughly addresses the risks associated with computer usage for these students. It is essential that students in grades K-12 be consistently exposed to curriculum regarding cyber-education in order to protect them from becoming victims of cybercrime as well as to prevent them from engaging in cybercrime. In addressing this issue, many schools and state legislatures have introduced various programs in the disciplines of technology and computer science.

Schools provide the optimal atmosphere for students to learn the essentials of cyber-safety and cyber-ethics, as they have consistent access to students during the most crucial years in their behavioral development (Sherman, Farrington, Welsh, & MacKenzie, 2002, pg. 56). However, without a standard curriculum in place, it is unlikely that all students in grades K-12 are receiving adequate educational information in regards to cybersecurity and cybercrime. For example, the 2011 *State of K-12 Cyberethics, Cybersafety and Cybersecurity Curriculum in the United States* report provided by the National Cyber Security Alliance (NCSA) displays survey data collected from over 1,000 individuals in charge of various educational positions in schools across the United States. The results of this survey exhibit that most teachers, administrators, and technology coordinators believe that cyber-education should be part of the curriculum in schools. Despite this agreement, it was also reported that the majority of schools surveyed do not require that cyberethics, cybersafety, or cybersecurity curriculums be taught in the classroom setting. Additionally, many of the teachers surveyed reported that they had not taught any topics essential to cyberethics, cybersafety, or cybersecurity in the past year. (NCSA, 2011). These

findings are concerning because they demonstrate that the demand for education in cybersecurity is not effectively being met in K-12 programs.

With the pressure of technology and the potential of cybercrime on the rise, it is essential to address the necessary resources and lessons required to run an effective cybersecurity program for grades K-12. While the increasing occurrence of cybercrime incidents in schools has created a demand for more cybersecurity education, few studies have been conducted to review existing programs and their effectiveness. Thus, the purpose of this study is to systematically evaluate existing cybersecurity education programs and describe their applications in creating an optimal cybersecurity curricular program.

The theoretical framework of this study will follow that of Choi's Cyber Routine Activities Theory (Cyber RAT). This theory states that while motivated offenders and suitable targets are always present online, the major factors impacting cybercrime occurrence are online lifestyle and digital capable guardianship. For the sake of this study, the computer hygiene category represents the online lifestyle described in Cyber RAT and technological skills provide the basis for capable guardianship. An additional consideration outside of the theoretical framework will be made for a computer ethics category.

This paper will include a review of the literature pertaining to the prevalence of cybercrime, its implications, and needs for more preventative measures through education. The literature review will be followed by a discussion of the methods used and of the findings resulting from this study. Finally, it will identify particular topics that should be included in an optimal K-12 cybersecurity program and will discuss how such a program should be implemented.

# LITERATURE REVIEW

## Theoretical Framework

Cybercrime has been defined as "any unauthorized, or deviant, or illegal activity over the Internet that involves a computer (or computers) as a tool to commit the activity and a computer (or computers) as the target of that activity" (Moitra, 2005, p.445). Cybercrime involves the use of both a network (such as the Internet) as well as a computer (Moitra, 2004, p.439). As new technology is developed, the threat of cybercrime increases and managing it becomes increasingly difficult. According to recent data, 48% of malicious email attachments were Microsoft Office files, putting Office software users at high risk of becoming victims. In 2018, it was also found that "1 in 10 URLs analyzed were identified as being malicious" and there was a 56% increase in web attacks overall. (Symantec, 2019). Additionally, recent research has reported that 69.9 percent of adolescents have experienced cyber-harassment at some point in their lives (Choi & Lee, 2017). However, cybercrime is extremely difficult to investigate and prosecute because, in many cases, it lacks a distinct jurisdiction due to its being committed through the Internet (Choi & Lee, 2017).

Despite the lack of enforcement against cybercrime, society's dependency on technology continues to increase, providing cybercriminals with increased opportunities to engage in crime (Choi, 2008). One theory that describes the prevalence of cybercrime is *Cyber Routine Activities Theory*, which is based on Cohen and Felson's 1979 *Routine Activities Theory* as well as Hindelang, Gotfredson, and Garofalo's 1978 *Life-Exposure Theory*. This adaptation of these theories states that in cyberspace, motivated offenders and suitable targets are assumed situational factors, therefore the availability of a capable guardian controls the probability of cybercrime victimization (Choi, 2008). According to this theory, the presence of a capable

guardian (such as computer protection software) and one's online lifestyle determines the likeliness of becoming a victim of cybercrime (Choi, 2008).

Cyber RAT in particular concentrates on "individuals' daily patterns of routine activities, including vocational activities and leisure activities, in cyberspace that increase the potential for computer crime victimization." The theory additionally considers "how computer security, as an important capable guardian in cyberspace, plays a major role against computer-crime victimization" (Choi, 2008). Digital guardianship is defined primarily in terms of protective measures available to Internet users such as antivirus software, antispyware software, and firewalls. On the other hand, online lifestyle is identified by "(a) vocational and leisure activities on the Internet, (b) online risky leisure activities, [and] (c) online risky vocational activities". (Choi, 2008).

**Cybersecurity Threats in Schools**

In 2018, there were 122 publicly reported cybersecurity incidents in K-12 schools throughout the United States. The majority of these incidents put students' personal information in jeopardy and was caused by the staff members or students at the schools. (Herold, 2019). Recent statistics show that "a U.S. school district becomes the victim of a cyberattack almost as often as every three days" (Security, 2019). Melissa Tebbenkamp, the director of instructional technology for Raytown Quality Schools, stated in an interview that the largest risk for cybersecurity in schools are the students and the school staff. Students become a risk factor when they are particularly knowledgeable about computers and purposely try to gain access to school data. On the other hand, school staff becomes more of a cybersecurity issue when it comes to opening emails or clicking on links intended to infect a computer with malware or phish for student information (Cavanagh, 2019). When student records are accessed by

unauthorized users, students become at risk for being approached online by predators (Cavanagh, 2019).

Students may also become a threat to cybersecurity in schools because "when children cannot validate the physical location or identity of an individual on the other end of the message, they may believe that their activity causes no perceptible harm and that there is limited chance for detection or punishment" (Berson & Berson, 2003, p.164-165). However, some cases prove that cybercrimes do not always provide complete anonymity for those students who choose to engage in them. An example of such a case is that of Jeremy Currier and Seth Stephens, who, for over a period of two years, gained unauthorized access to their school district's computer systems and information such as logins, passwords, phone numbers, locker combinations, lunch balances, and grades of other students (Herold, 2018). Though the teenagers were eventually caught and expelled for their actions, this incident, as well as many others, has demonstrated the weak cybersecurity practices in many school districts that put them at risk for falling victim to cybercrime (Herold, 2018).

**K-12 Cybersecurity Program: Major Components**

The most effective way to protect K-12 students from dangerous and inappropriate online content is through education of how to be an ethical digital citizen (Berson & Berson, 2003, p.164). Most children are uninformed in regards to the dangers of computer and Internet use, making them easy targets for cyberattacks. As a result, there has been an increase in cyber safety materials becoming available online. However, these materials "work on a voluntary basis and so aren't viable to ensure measureable mass adoption" (Saluja, Bansal, & Saluja, 2012). The most effective way to ensure that this information is spread to all students is through its implementation in schools (Saluja, Bansal, & Saluja, 2012). Because schools have consistent,

mandated access to children during the most crucial periods of their behavioral development, these institutions have great potential in promoting cybersecurity prevention through education (Sherman, Farrington, Welsh, & MacKenzie, 2002, p.56).

It is imperative that, in addition to education, schools develop and implement a plan that focuses on preventing and handling threats to their cybersecurity (Levin, 2019). These plans should include features such as firewalls, virus protection, consistent user training for staff, restricting administrative access (meaning preventing school staff from downloading software), and backing up data (Cavanagh, 2019). Implementing these various methods of computer security will provide schools with the strong capable guardian needed to protect against cybercrime victimization and will promote the application of a safer online lifestyle. Essentially, in order to reduce computer-crime victimization, "pro-social views of promoting adequate online lifestyle and utilizing efficient computer security" must be established (Choi, 2008).

**Israeli Cyber-Education**

Israel has been a world leader in cybersecurity and cyber-technology for many years. However, the Israeli government has just recently invested a great deal of resources into cyber education. For example, the Magshimim program allows 10$^{th}$ graders to "take after-school classes in encryption, coding, and preventing malicious hacking" (Kfir, 2018). Another new program that was initiated during this school year focused on training 100 seniors to become computer hackers and 240 to become cyber protectors. Facilitators of this program include cyber-technology and cyber warfare experts. The program additionally incorporates "extensive instruction on ethics and 'permissible and prohibited conduct in the field'" (Barrow, 2018). In addition to the government sponsoring cyber education programs for Israeli youth, the private sectors have been involved in "recruit[ing] engineers and programmers to teach in schools,

organiz[ing] tours of technology companies for school kids, and help[ing] the volunteer teachers get jobs in technology companies" (Press, 2017).

**Learning by Doing**

History has demonstrated that knowledge and the application of knowledge are crucial factors involved in learning and developing. Essentially, this means that the act of "doing" increases the effectiveness of learning outcomes. Thus, programs should "identify that students need to have an understanding of and be able to use what they learn (the doing) to be literate in a particular subject matter." The *Learning by Doing* study has found that "teachers feel that students benefit from doing activities in their classrooms" and that "middle school students are doing more activities and projects than are elementary and high school students." Overall, this research has determined that "learning by doing was confirmed as an essential, but underutilized, method of learning" (Moye, Dugger & Stark-Weather, 2014).

**Synopsis of K-12 Cybersecurity Education in the Past**

Approximately half of students in 12$^{th}$ grade do not have access to computer science courses while in high school, demonstrating how computer education is not emphasized in many standards guiding curriculum in state schools, and therefore receives limited funding (Chatlani, 2017). Results from the 2011 *State of K-12 Cyberethics, Cybersafety and Cybersecurity Curriculum in the United States* survey have demonstrated significant trends in the perspectives of over 1,000 teachers, administrators, and technology coordinators at schools regarding how cybersecurity is taught in their school districts. Although 91% of teachers in the surveyed districts believed that cyberethics, cybersafety, and cybersecurity should be taught in schools, only 51% reported that their school or district did an adequate job of preparing their students in these issues. Furthermore, only 29% stated that their school or district required a cyberethics

curriculum, 33% stated that their school or district required a cybersafety curriculum, and 30% stated that their school or district required a cybersecurity curriculum. Additionally, 76% of teachers only had up to three hours of cybersecurity training in their school or district in the past 12 months. Most teachers (79%) also reported that they believed parents were most responsible for teaching their children to use computers safely and securely, whereas only 18% found themselves to be most responsible (StaySafeOnline.org, 2011).

**Computer Hygiene.** Cybersafety is one of the most important focus areas in the computer hygiene category. Cybersafety was defined by the 2011 survey as "Warning signs to let your parents know about", "The risks tied to social networking sites", "How to make decisions about sharing personal information on the Internet", "Watching out for online predators", "What to do if you or someone you know receives inappropriate or harassing messages", "What to do if someone posts unwanted or inappropriate material", "The value of privacy and personal information and your responsibility for protecting the information and reputations of friends, family, and others online", "Scams, fraud, and social engineering", "The safe use of geo-location services", "Sexting of the inappropriate sharing of sexually suggestive images", "Other", "None", and "Not sure". In regards to teaching cybersafety, 41% of teachers reported that "None" of these topics had been taught in the past year, which was the highest of all of the topics selected for this portion of the survey. The least selected topics were "Warning signs to let your parents know about" (17%), "Sexting" (17%), and "The safe use of geo-location services" (6%). (StaySafeOnline.org, 2011).

An additional core educational component described as computer hygiene is the management of computer security. The topics listed for education in cybersecurity included "Using strong passwords", "Changing passwords often", "Knowing when it is safe to download

a file", "Risks associated with peer-to-peer networks", "How to identify a secure Web site", "Identity theft", "Protecting computers from malicious software", "The role of a more secure Internet in our economy", "The role of a more secure Internet in our national security", "Protecting a mobile device", "Careers in cybersecurity", "Other", "None", and "Not sure". Again, the majority teachers (50%) reported that "None" of the above topics had been taught in the past year. The least taught topics included "Protecting computers from malicious software" (15%), "The role of a more secure Internet in our economy/ national security" (7% and 6%, respectively), "Protecting a mobile device" (6%), and "Careers in cybersecurity" (4%). (StaySafeOnline.org, 2011).

**Cyberethics.** The survey mentioned above questioned teachers about what topics in cyberethics they had taught students in the past year. These topics included: "Dealing with posts, videos, or other web content that scares you", "How to send an email", "Respecting the privacy of others", "Exercising proper 'netiquette', or knowing how to conduct one's self while online that is appropriate and courteous to others", "Hacking, or gaining access to a computer file or network without authorization", "Plagiarism", "Downloading (legally or illegally) music and video files", "Dealing with posts, videos or other Web content that contain 'hate speech'", "Other", "None", and "Not sure". Notably, 32% of the respondents selected "None" in this category, which only fell behind "Plagiarism" (47%) and "Respecting the privacy of others" (33%) in regards to the most frequently taught cyberethics topics. "Hacking, or gaining access to a computer file or network without authorization" was only selected by 8% of the respondents. (StaySafeOnline.org, 2011).

Emphasizing legal issues in cybercrime is an essential way to promote cyberethics. Although it is recognized that cybercrime is a serious issue that needs to be addressed in law and

law enforcement, not enough information is known about cybercrime to establish adequate policies or laws in regards to the issue (Moitra, 2005, p.463). However, a federal act was developed in 2018 to form the Cybersecurity and Infrastructure Security Agency (CISA), an expansion of the Department of Homeland Security. This agency was created to "help the U.S. government address current security gaps", such as by collecting data on trends in cybercrime (HIPPA Journal, 2018).

There have been more than 265 bills from various states introduced or considered in the United States in regards to cybersecurity; however, only about 52 of them have been enacted thus far and of those enacted, none have involved the implementation of mandatory K-12 educational programs (Cybersecurity Legislation, 2018). The only state that has truly addressed the issue of cybersecurity education in law to date is California, which has enacted the *Cyber Secure Youth Act*. The Cyber Secure Youth Act requires that school districts in California teach students cyber-hygiene at least once during their K-6 education and again in grades 7-12. The act defines cyber-hygiene as online account maintenance, safe online behavior, computer literacy, and community responsibility (Good Day Sacramento, 2018).

## METHODS

### Search Strategies

Due to a lack of peer-reviewed articles regarding K-12 cybersecurity educational programs, a basic Google search was used to locate relevant programs uploaded online by various schools, districts, states, and private corporations. The following search items were combined to conduct the search: cybersecurity education K-12, K-12 cybersecurity programs, curriculum, state cybersecurity standards, and computer education K-12. As a result, a total of 96 programs were identified and reviewed for information relevant to this study. Programs were

further selected if they included specific information regarding the teaching of cybersecurity essentials in K-12 educational settings.

**Data Collection**

Information was collected from each relevant program according to a checklist drafted purposely for this study. The checklist included specific sections for demographic information, computer hygiene implementations, computer ethics implementations, and technological skills implementations in accordance with the Cyber RAT theoretical framework. Topics included in computer hygiene were whether each of programs address “The importance of updating antivirus software”, “How to install antivirus software”, “How to create and maintain strong passwords”, “Malware protection”, “Firewalls”, “Social media use”, “Cybersecurity monitoring”, “Site credibility”, “Cyber incident reporting”, “Cleaning up web history”, and “Cookies”. Under computer ethics, the topics covered were “Copyright laws”, “Downloading materials from the web”, “Hacking”, “Computer/Cyber Laws”, “Cyberbullying”, “Responsible use policies”, and “Darknet”. Lastly, technological skills incorporated “Coding basics”, “Operating systems basics”, “Information technology”, “Networking”, “Encryption”, “Digital forensics”, “Cryptography”, “Database usage”, “Penetration testing”, “Search engine usage”, “Cryptocurrency”, “Computer parts”, “Keyboarding”, “Word processing”, and “Multimedia”. Technological skills were further divided into specific coding languages such as Python, Java, Javascript, C++, Scratch, and HTML and into the specific operating systems of Windows, Mac, and Linux. All three categories additionally included checklist sections for methods used to teach the topics and for who was responsible for facilitating the category. See **Appendix A** for the full survey.

**Analytical Strategy**

Each question of the checklist shown in **Appendix A** was coded into the SPSS statistical software for further evaluation. Utilizing this software, data trends were recorded in regards to the frequency of each element item used within the programs as well as trends across each discipline. The total elements used in each of the three main sections (computer hygiene, computer ethics, and technological skills) were demonstrated individually in frequency charts and in histograms to assess the effectiveness of each program at addressing these issues. Finally, all three elements of total computer hygiene, computer ethics, and technological skills were combined into a total cybersecurity histogram, representing the amount of topics covered in educational cybersecurity programs as a whole. Furthermore, correlations were tested for significance between particular survey items using regression analysis and Chi-Square tests. Coefficients tables were used in SPSS to describe significance between variables.

## KEY FINDINGS

### Demographics

The demographic information regarding the programs in this study is shown in Table 1 below. The majority of the programs utilized for this study were state mandated standards for computer science and technology. Most were also designed to run throughout the total duration of each student's K-12 education and were either specifically targeted at grades 1-5 or focused on all grades. All 96 programs also required additional resources to accompany the program facilitators.

**Table 1. Program Demographics (N = 96)**

| Variable | n | n(%) |
|---|---|---|
| **Ownership** | | |
| School | 11 | 11.5 |
| Corporation Sponsored | 14 | 14.6 |
| District Owned | 25 | 26 |

| | | |
|---|---|---|
| State Owned | 46 | 47.9 |
| **Program Duration** | | |
| 1 Week | 1 | 1.1 |
| 1 Month | 2 | 2.1 |
| 1 Year | 22 | 23.2 |
| All Years | 70 | 73.7 |
| **Target Participant Age** | | |
| Kindergarten | 1 | 1 |
| Grades 1-5 | 31 | 32.3 |
| Grades 6-8 | 17 | 17.7 |
| Grades 9-12 | 16 | 16.7 |
| All K-12 | 31 | 32.3 |
| **Mandatory** | | |
| No | 18 | 18.8 |
| Yes | 78 | 81.3 |
| **Facilitators** | | |
| Teacher | 86 | 89.6 |
| IT Staff | 41 | 42.7 |
| Administration | 0 | 0 |
| College Professor | 0 | 0 |
| Online Resource Only | 11 | 11.5 |
| **Resource Requirements** | | |
| Computer Access | 96 | 100 |
| Online Access | 96 | 100 |
| Software Installation | 87 | 90.6 |
| Computer Specialists | 40 | 41.7 |

**Computer Hygiene**

From the frequency table (Table 2) of topics covered in computer hygiene, the top three topics taught in the programs were:

1) *Cybersecurity Monitoring*, which included recognizing signs of cyberattacks and managing a strong protection against them.
2) *Site Credibility*, which included recognizing and using secure and reputable websites while online.

3) *Passwords*, which included creating strong passwords, consistently changing passwords, and protecting passwords.

**Table 2. Computer Hygiene Topics (N=96)**

| Variable | n | n(%) |
|---|---|---|
| Antivirus Update | 31 | 32.3 |
| Antivirus Install | 30 | 31.3 |
| **Passwords** | **57** | **59.4** |
| Malware Protection | 40 | 41.7 |
| Firewalls | 13 | 13.5 |
| Social Media | 45 | 46.9 |
| **Cybersecurity Monitoring** | **74** | **77.1** |
| **Site Credibility** | **62** | **64.6** |
| Incident Reporting | 45 | 46.9 |
| Cleaning Web History | 22 | 22.9 |
| Cookies | 12 | 12.5 |

Total computer hygiene was computed by combining all elements of computer hygiene and measuring the frequencies with which they were covered in all 96 programs. The mean number of computer hygiene topics taught was 4.5 with a standard deviation of 2.3, a maximum of 10, and a minimum of 1 (See **Appendix B**).

The topic of computer hygiene was taught primarily in the form of lectures (96.9%) and discussions (92.7%). Online resources and hands-on activities were only utilized 13.5% and

30.2 % of the time, respectively. Content teachers (88.5%) and specific IT staff instructors (41.7%) were responsible for teaching the material to students.

**Computer Ethics**

From the frequency table (Table 3) of topics covered in computer ethics, the top three topics taught included:

1) *Copyright Laws*, including laws against plagiarism and how to cite sources for research.
2) *Computer/Cyber Laws*, including laws against crimes committed online and penalties for breaking such laws.
3) *Responsible Use Policies*, including policies regarding the proper use of school owned technology or online programs.

**Table 3. Computer Ethics Topics (N=96)**

| Variable | n | n(%) |
|---|---|---|
| **Copyright Laws** | **71** | **74** |
| Downloading web materials | 44 | 45.8 |
| Hacking | 33 | 34.4 |
| **Computer/Cyber Laws** | **62** | **64.6** |
| Cyberbullying | 49 | 51 |
| **Responsible Use Policies** | **61** | **63.5** |
| Darknet/TOR Browser | 3 | 3.1 |

Total computer ethics was computed by combining all elements of computer ethics and measuring the frequencies with which they were covered in all programs. The mean number of

topics taught in this category was 3.36, with a standard deviation of 1.36, a maximum of 6, and a minimum of 1 (See **Appendix C**).

**Technological Skills**

From the frequency table (Table 4) of topics covered in technological skills, the top three topics taught were:

1) *Coding Basics*, which included binary numbers, algorithms, and programming languages.
2) *Computer Parts*, which included identifying and locating specific components of computer devices.
3) *Database Usage*, which included searching databases for research and creating databases for collected data.

**Table 4. Technological Skills Topics (N=96)**

| Variable | n | n(%) |
|---|---|---|
| **Coding Basics** | **68** | **70.8** |
| Operating Systems Basics | 39 | 40.6 |
| Information Technology | 40 | 41.7 |
| Networking | 49 | 51 |
| Encryption | 36 | 37.5 |
| Digital Forensics | 3 | 3.1 |
| Cryptography | 13 | 13.5 |
| **Database Usage** | **52** | **54.2** |
| Penetration Testing | 1 | 1 |
| Search Engines | 50 | 52.1 |
| Cryptocurrency | 1 | 1 |

| | | |
|---|---|---|
| **Computer Parts** | **55** | **57.3** |
| Keyboarding | 18 | 18.8 |
| Word Processing | 40 | 41.7 |
| Multimedia | 35 | 36.5 |

The total of technological skills was computed by combining all elements of the technological skills category and measuring the frequencies with which they were covered in the programs. The mean number of technological skills topics taught was 5.21, with a standard deviation of 2.49, a maximum of 12, and a minimum of 1 (See **Appendix D**).

Although listed on the survey, there was an insignificant amount of information found in regards to the specific computer systems and operating systems discussed in the programs. If mentioned at all in the program frameworks, the most common form of coding language utilized was a basic block-based language, such as Scratch (33.3%).

In regards to how topics of technological skills were taught in the programs, the most common were again lecture (97.9%) and discussion (84.4%). However, hands-on activities or labs were also used frequently (67.7%) and online resources were utilized in 35% of programs. School teachers (90.6%) and IT staff instructors (44.8%) were again the primary sources of instruction for these materials.

**Total Cybersecurity**

Total cybersecurity was a measurement of the total number of topics taught overall with all three categories combined. The mean number of total topics covered was 13.78, with a standard deviation of 5.12, a maximum of 28, and a minimum of 5 (See **Appendix E**).

**Cross-Evaluations**

**Mandated Programs and Program Ownership.** Prior to viewing the findings of this study, it was hypothesized that there would be a significant correlation between whether or not a program was mandatory and the ownership of the program. This hypothesis was based on the belief that school, district, or state-owned programs would be mandated in K-12 education, whereas online, corporation-sponsored programs would only be available on a voluntary basis.

**Table 5. Mandatory Program and Program Ownership.**

| Variable | Value | df | Asymp. Sig. (2-sided) |
|---|---|---|---|
| Pearson Chi-Square | 73.181 | 3 | .000*** |

*** = p< .05, ** = p< .01, *** = p< .001**

Whether or not a program is mandatory and the ownership of a program has a strong, statistically significant correlation, as demonstrated in the results of a Chi-Square test comparing the two variables. The significance value for this test was .000, showing a high correlation. As can be seen in **Appendix F**, programs that are school owned, district owned, or state owned are for the most part mandatory, whereas corporation-sponsored programs are not necessarily mandatory.

**Total Program Effectiveness Correlations.** It was initially hypothesized that more topics would be covered in programs with longer durations because there would be more time available to cover a larger range of material. It was additionally believed that hands-on activities would increase the effectiveness of the program because it allows students to apply their knowledge. Lastly, it was expected that there would be a significant relationship between the number of topics taught and the program facilitator because it is assumed that the more experience the instructor has, the more topics that can be covered.

**Table 6. Total Effectiveness**

| Variable | Mean | Std. Deviation | ß | Sig. |
|---|---|---|---|---|
| Program Duration | 4.76 | 0.43 | 0.510 | 0.004** |
| Method of Teaching | | | | |
| Handout/Lab | 0.677 | 0.470 | 0.374 | 0.000*** |
| Discussion | 0.844 | 0.365 | 0.207 | 0.031* |
| Program Facilitators | | | | |
| School Teacher | 0.906 | 0.293 | 0.237 | 0.015* |
| IT Staff | 0.448 | 0.499 | 0.483 | 0.000*** |

*** = p< .05, ** = p< .01, *** = p< .001**

The duration of the program was only found to be statistically significant in regards to the teaching of technological skills. Table 6 demonstrates this significant relationship with a Sig. p-value of .004. The value of B for this correlation is 2.949, demonstrating an increase of technological skills teaching effectiveness (total technological skills score) by up to almost 3 points for an increase in duration time. (See **Appendix F**).

The method by which topics were taught was also only statistically significant in the technological skills category. As shown in Table 6, technological skills were most effective when taught using a handout or lab exercise (Sig. p-value = .000). The B value for this topic was 1.981, meaning the teaching effectiveness (total technological skills score) increased by almost 2 points when taught using a handout or lab activity. (See **Appendix F**).

The score of effectiveness for the teaching of technological skills in a program was also significantly impacted by who was facilitating the instruction. Table 6 shows that incorporating IT staff as facilitators significantly increases the effectiveness of teaching technological skills (Sig. p-value = .000) by approximately 2 score values (B = 2.402). (See **Appendix F**).

## DISCUSSION

Based on the 2011 *State of K-12 Cyberethics, Cybersafety and Cybersecurity Curriculum in the United States* study, it was predicted that most programs would not sufficiently cover topics regarding computer hygiene, ethics, or technological skills. However, our findings show that, on average, most programs cover roughly half of the necessary topics. These findings suggest that the statistics from 2011 may have improved in recent years.

As demonstrated in the frequencies at which specific topics were taught in the cyber-hygiene category, the majority of programs covered cybersecurity monitoring, site credibility, and creating strong passwords. These programs rarely included instruction regarding firewalls and cookie use. For cyber-ethics, most programs included copyright laws, computer and cyber laws, and responsible use policies, whereas the darknet and TOR browser were barely discussed. In terms of technological skills, the most frequent topics taught were coding basics, computer parts, database usage, and search engines. Programs did not significantly cover the topics of cryptocurrency, penetration testing, or digital forensics.

Based off of the frequencies of the topics taught in the programs alone, it is clear that the majority of program developers find importance in including the topics mentioned above in K-12 cybersecurity educational curriculums. An interesting observation about these findings is that some of the most frequently taught subjects (site credibility, copyright law, databases, and search engines) are important aspects of researching and writing academic papers, which might explain why they are so commonly demonstrated at the K-12 level. The topics that were not heavily taught in the programs (darknet/TOR, cryptocurrency, penetration testing, and digital forensics) may be a wise decision on the program developers' part because these aspects are rather advanced and students at the K-12 level may not be prepared to understand the negative implications that some of them include.

**Recommendations and Policy Implications**

As discussed previously, it seems as though most programs are concerned with teaching students necessary research skills for academic writing. Thus, we recommend that programs include a stronger focus on teaching topics that will help protect students from becoming victims of cybercrimes, prevent them from engaging in cybercriminal acts, and allow them to explore potential careers in the cybersecurity field. This would entail a shift to teaching more about coding, malware and virus protections, incident reporting, download safety, information technology, and operating systems. Although topics involved in academic writing (copyright law, site credibility, word processing, etc.) should not be ignored in K-12 education, it is important to also incorporate more lessons directly related to cybersecurity.

The threat of cybercrime continues to grow as technological advancement increases, creating a higher demand for preventing such crimes and for hiring cybersecurity professionals. Cybercrime is especially prevalent in schools, making it even more necessary to teach students to engage in ethical cyber behaviors and to protect themselves in the digital world. Thus, an ideal cybersecurity education program should be centered on topics that aim to protect against and prevent cybercrime occurrences.

In future programs, it would additionally be worthwhile to include more hands-on activities in all realms of cybersecurity education to determine if their effect would be significant on the effectiveness of teaching computer hygiene and ethics as they were in technological skills. As discussed in the *Learning by Doing* subsection of the literature review in this study, hands-on activities are imperative to the learning process by allowing students to apply their knowledge to a given task. Our findings also show that there is a correlation between programs that cover a

high number of topics and those that use hands on methods, further supporting the notion to increase the use of hands-on methods of teaching.

According to the findings, technological skills were most effectively taught in programs with longer durations. As a result, an ideal cybersecurity educational program should run throughout the entire duration of a student's K-12 education experience. By including a program into a school's curriculum for each grade level in K-12, students will be able to effectively build on knowledge from previous years and will have consistent exposure to topics in cybersecurity.

As revealed in the findings, cybersecurity programs are most frequently instructed by content teachers and specialized IT staff instructors. However, programs that utilized IT staff instruction prevailed at effectively covering aspects of technological skills. These findings indicate that an ideal cybersecurity educational program should be facilitated using the instruction of content teachers, but should also include specialized IT staff instructors.

It is sensible to have instructors on staff that has been trained specifically in technological skills to teach cybersecurity to students because their background knowledge includes topics specific to this discipline. Ultimately, these staff members would be more equipped to teach students skills needed to be technologically successful. Furthermore, it may be interesting to include field specialists or college professors in facilitating the instruction, as they may be able to provide even more knowledge than content teachers or IT staff. Examples of this are seen in the successful Israeli cyber educational framework, where resources are spent hiring instructors who have high levels of field experience.

Parents of students may also play a significant role in securing their children's online lifestyle behavior and serving as a capable guardian. Because of this, it is recommended that

schools offer parental management and reinforcement courses in order to maintain students' safe online practices while they are at home as well as in school.

Law enforcement officials may also take part in the implementation of cyber education programs, as it is necessary to build community trust for cybercrime reporting in the same way as traditional crime. Policies during the implementation of these programs could additionally include training for law enforcement to help them with identifying, protecting against, and dealing with cybercrime.

It is further recommended that cyber education programs be made into mandatory core curriculum classes for all students in grades K-12 so that it is ensured that they have continuous and consistent exposure to the material. Once all of the necessary aspects of an optimal K-12 cybersecurity education program have been identified, policy could be proposed to the United States government to make these aspects a global standard for all schools to include into their core curriculum (such as is already the case with math, science, language arts, and history classes). This policy would require that cybersecurity fundamentals be taught in all K-12 programs so that students would receive and build upon knowledge to help them become well-rounded digital citizens and would maintain a structured program that does not fluctuate from school to school. In order to effectively implement such programs, governmental support would be necessary, especially to assist with program funding for public institutions. It would be beneficial for the United States to follow the already established Israeli cyber education framework, in which the government provides funding for resources needed to train students to work in the field of cybersecurity.

In future studies, it would be beneficial to collect qualitative data in the form of interviews and observation of the programs in action to determine whether or not the quality of

the programs adequately addresses the necessary components of cybersecurity education. Overall, such a study would assess the effectiveness of the programs on preventing students from becoming victims of cybercrime or from committing cybercrimes. Other studies on this topic may include actually drafting an optimal K-12 cybersecurity educational program from the standards listed in this study, implementing the program in various schools, and measuring the program's short-term and long-term successes of preventing cybercrime.

**Limitations**

This study was highly exploratory in nature with the intentions of determining crucial aspects needed to create an ideal cybersecurity education program for students in grades K-12; however, some limitations to this research are present. First, the number of programs studied in this research may not be sufficient or representative of all programs that exist in schools in the United States. During the search process, some schools had program curriculums posted online that could not be accessed without a specific username or password for that particular school. As a result, these programs were not included in the collection of data for this research. This may have impacted our overall results by limiting our data only to programs that could be easily accessed online.

Second, in some cases, program syllabi may not have provided a sufficient amount of in depth information regarding all features of the program, meaning that these aspects may simply not have been specified despite being used in the program. For example, some programs may utilize specific teaching methods such as lab activities or may be facilitated by college professors, but may not include these characteristics in the program framework. The implication this limitation has on our data is that it may not allow us to fully encompass every feature that each program entails.

Lastly, it is remotely impossible to completely know how truly effective each program is at teaching the topics of cybersecurity or preventing cybercrime without actually observing the programs in action or collecting data from students who had and had not participated in the program. A more qualitative approach in the form of interviews, observations, or surveys would be more apt to provide information regarding the adequacy and overall effectiveness of the programs. However, this data may potentially be collected in future studies that are intended to look more closely at overall program effectiveness.

## CONCLUSION

Although research on incorporating cybersecurity education into the K-12 framework is still in its early stages, it is essential to recognize the importance of these programs to the overall prevention of cybercrime in the years to come. Our findings suggest that while some schools or states have implemented some topics of cybersecurity into their core curriculum, it is necessary to apply a more narrow focus on teaching computer hygiene, computer ethics, and technological skills to students. As discussed previously, these topics fit into the Cyber RAT theoretical framework by teaching safe online lifestyles (computer hygiene) and providing digital capable guardianship (technological skills). As this theory has been applied to cybercrime prevention practices, focusing on these topics with the addition of computer ethics will further allow students to explore relevant issues in cybersecurity and will protect them from becoming victims or criminals of cybercrime. Education is the means by which we all broaden our understanding of various subjects throughout our lives, grades K-12 being the peak years in which we have access to consistent, mandated exposure to education. Just as school systems maintain core curriculums of Language Arts, History, Math, and Science to prepare students for various professional experiences, they should begin to introduce cybersecurity into the core curriculum

as well to prepare them for the digital world. This study contributes to increasing the understanding of the importance of implementing cybersecurity education in grades K-12 and to how these programs should be evaluated for overall effectiveness.

## REFERENCES

2016 Massachusetts Digital Literacy and Computer Science ... (2016). Retrieved from http://www.doe.mass.edu/frameworks/dlcs.pdf

2020 Colorado Academic Standards Downloads. (2018). Retrieved from http://www.cde.state.co.us/standardsandinstruction/standards

Alabama State Department of Education. (2018). Digital Literacy and Computer Science. Retrieved from https://www.alex.state.al.us/browseDLIT.php

Arizona Computer Science Standards Development. (2018). Retrieved from http://www.azed.gov/standards-practices/arizona-computer-science-standards-dev/

Barrow, T. (2018, August 13). How Israel Is Raising up a Generation of 'Cyber Warriors'. Retrieved from https://www1.cbn.com/cbnnews/israel/2018/august/israeli-school-kids-will-train-to-be-cyber-warriors

Berson, I. R., & Berson, M. J. (2003). Digital Literacy for Effective Citizenship. *Social Education*,*67*(3), 164-167.

Cavanagh, S. (2019, March 19). The Best Defense Against Cyberattacks, From a District CTO. Retrieved from https://www.edweek.org/ew/articles/technology/2019/03/20/the-best-defense-against-cyberattacks-from-a.html

Cavanagh, S. (2019, March 19). 6 Steps for Preventing and Cleaning Up Cyberattacks. Retrieved from https://www.edweek.org/ew/articles/technology/2019/03/20/6-steps-for-preventing-and-cleaning-up.html

Chatlani, S. (2017, November 02). It's time to address cybersecurity education, say policymakers. Retrieved from https://www.educationdive.com/news/its-time-to-address-cybersecurity-education-say-policymakers/509740/

Choi, K., & Lee, J. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior,*394-402.

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology,2*(1), 308-333.

Cleburne Independent School district. (2018). Retrieved from https://www.cleburne.k12.tx.us/apps/pages/index.jsp?uREC_ID=301609&type=d&pREC_ID=892780

Computer Science 7-12 Program Guidelines - education.pa.gov. (2018, December). Retrieved from https://www.education.pa.gov/Documents/Teachers-Administrators/Certification Preparation Programs/Specific Program Guidelines/Computer Science 7-12 Program Guidelines.pdf

Computer Science Courses. (n.d.). Retrieved from http://ohs.rsu13.org/cs#ecsexploring computer science rockland

Computer Science Education. (2018). Retrieved from https://www.cde.ca.gov/be/st/ss/computerscicontentstds.asp

Computer Science for Cyber Security (CS4CS). (n.d.). Retrieved from https://engineering.nyu.edu/research-innovation/k12-stem-education/student-programs/computer-science-cyber-security-cs4cs

Computer Science Performance Standards K-12 (2019). (2019). Retrieved from https://dese.mo.gov/sites/default/files/curr-mls-standards-computer-science-k-12-sboe-2019.pdf

Computer Science Standards. (n.d.). Retrieved from https://sde.ok.gov/computer-science-standards

Computer Science Standards and Courses. (2016). Retrieved from http://www.arkansased.gov/divisions/learning-services/curriculum-and-instruction/curriculum-framework-documents/computer-science

H. (2018, November 15). Congress Passes CISA Act: New Cybersecurity Agency to be Formed within DHS.

CSTA Computer Science Standards. (2011). Retrieved from https://www.csteachers.org/page/standards

CT Computer Science Implementation Guidelines. (2018). Retrieved from https://portal.ct.gov/-/media/SDE/Computer-Science/Connecticut_Computer_Science_Implementation_Guidelines.pdf?la=en

Curriculum / Technology. (2018). Retrieved from https://www.tumwater.k12.wa.us/Page/2967

Curriculum Guides / Technology. (2011). Retrieved from https://www.k12northstar.org/Page/2937

Curriculum Maps / Computer Literacy & Applications. (2012). Retrieved from https://www.somervillenjk12.org/Page/1563

Cyber Security Classes May Be Required In California Schools. (2018, June 26). Retrieved from https://sacramento.cbslocal.com/2018/06/26/cyber-security-classes-may-be-required-in-california-schools/

Cybersecurity in K-12 Education Syllabus. (2018). Retrieved from https://cosn.org/cybersecurity-k-12-education-syllabus

Cybersecurity Legislation 2018 - ncsl.org. (2018, February 8). Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx

Digital Citizenship. (2015). Retrieved from https://www.commonsense.org/education/digital-citizenship

Digital Readiness. (2018, March). Retrieved from https://www.tn.gov/content/dam/tn/stateboardofeducation/documents/2018_sbe_meetings/april_

20_2018_sbe_meeting/4-20-18 III G K-8 Computer Science Standards Attachment Clean Copy.pdf

Easy Steps Program. (2018, August 21). Retrieved from https://www.k12blueprint.com/publications/easy-steps

Exploring Computer Science. (2018). Retrieved from http://www.exploringcs.org/

Florida Standards Science – Computer Science Standards. (n.d.). Retrieved from http://www.cpalms.org/Standards/Computer_Science_Standards.aspx

Herold, B. (2019, February 7). Schools Suffered at Least 122 Cybersecurity Incidents Last Year. Retrieved from http://blogs.edweek.org/edweek/DigitalEducation/2019/02/schools_cybersecurity_incidents_2018.html

Herold, B. (2019, February 20). They Hacked Their School District When They Were 12. The Adults Are Still Trying to Catch Up. Retrieved from https://www.edweek.org/ew/articles/2018/11/07/they-hacked-their-school-district-when-they.html

Idaho K 12 Content Standards for Computer Science. (2018). Retrieved from https://stem.idaho.gov/wp-content/uploads/2018/01/IdahoK-12ContentComputerScienceStandards-TableFormat-OfficialVersion.pdf

Indiana K-12 Computer Science Standards - doe.in.gov. (2016). Retrieved from https://www.doe.in.gov/sites/default/files/wf-stem/indiana-k-12-computer-science-standards.pdf

INFORMATION AND TECHNOLOGY. (n.d.). Retrieved from http://www.ncpublicschools.org/curriculum/infotech/

ISTE Standards for Students. (2016). Retrieved from https://www.iste.org/standards/for-students

K-12 Computer Science Standards - Nevada Department of ... (2018, June). Retrieved from http://www.doe.nv.gov/Standards_Instructional_Support/Nevada_Academic_Standards/K_12_Computer_Science_Standards/

K-12 Curriculum. (2009). Retrieved from http://www.slcs.us/departments/administration_building/cita/k-12_curriculum.php

Kansas Computer Science Standards. (n.d.). Retrieved from https://www.ksde.org/Agency/Division-of-Learning-Services/Career-Standards-and-Assessment-Services/Content-Area-A-E/Computer-Science

Kentucky Academic Standards Computer Science. (n.d.). Retrieved from https://education.ky.gov/curriculum/standards/kyacadstand/Documents/Kentucky_Academic_Standards_Computer_Science.pdf

Kfir, I. (2018, November 04). Learning from Israel's cyber playbook. Retrieved from https://www.policyforum.net/learning-israels-cyber-playbook/

Learn Computer Science. (2018). Retrieved from https://studio.code.org/courses

Levin, D. (2019, March 19). Why K-12 Cybersecurity Is Only as Good as the Leadership at the Top. Retrieved from https://www.edweek.org/ew/articles/technology/2019/03/20/why-k-12-cybersecurity-is-only-as-good.html

Maryland's K-12 Computer Science Standards. (2018, September). Retrieved from https://msdecomputerscience.weebly.com/framework-and-standards.html

Mashburn, D. (2016). Curriculum: Technology. Retrieved from http://www.lbusd.k12.ca.us/Departments/Curriculum/Technology/curriculum_docs.cfm

Michigan K-12 Computer Science Standards - January 2019. (2019, January). Retrieved from https://www.michigan.gov/documents/mde/CompSci_Standards_Accessible_Final_Draft_642640_7.pdf

Midland Park Public SchoolsExcellence in Education. (2016). Retrieved from https://www.mpsnj.org/academics/curriculum/k-12_curriculum/technology_k-12

Mississippi College and Career-Ready Standards. (2018). Retrieved from https://mdek12.org/OAE/college-and-career-readiness-standards

Moitra, S. (2005). Developing Policies for Cybercrime. *European Journal of Crime, Criminal Law and Criminal Justice,13*(3), 435-464. doi:10.1163/1571817054604119

Montana K-12 Digital Literacy and Computer Science Guidelines. (2010, January). Retrieved from http://montanateach.org/wp-content/uploads/2018/07/DigitalLiteracyComputerScienceGuidelines-2018.pdf

Moye, J. J., Dugger, W. E., & Stark-Weather, K. N. (2014, September). "Learning by Doing" Research Introduction. Retrieved from https://www.iteea.org/Activities/2142/Learning_Better_by_Doing_Project/50026/39126.aspx

NBES Computer Lab Curriculum - Snoqualmie Valley School ... (n.d.). Retrieved from https://www.svsd410.org/site/handlers/filedownload.ashx?moduleinstanceid=9481&dataid=11883&FileName=NBES Computer Lab Curriculum.pdf

NEBRASKA K-12 TECHNOLOGY - cdn.education.ne.gov. (n.d.). Retrieved from https://cdn.education.ne.gov/wp-content/uploads/2018/04/NEK12Tech.pdf

New Jersey Core Curriculum Content Standards- Technology. (2014, October). Retrieved from https://www.nj.gov/education/cccs/1996/06artsintro.html

North Dakota Computer Science and Cybersecurity Standards ... (2019). Retrieved from https://www.nd.gov/dpi/uploads/87/2019ComputerScienceCybersecurity.pdf

Ohio's Learning Standards for Technology. (2017). Retrieved from http://education.ohio.gov/Topics/Learning-in-Ohio/Technology/Ohios-Learning-Standards-for-Technology

OtsegoElementary School. (2017). Retrieved from https://elementary.otsegoknights.org/apps/pages/index.jsp?uREC_ID=987702&type=d&pREC_ID=1304442

PLAINVIEW-OLD BETHPAGE CENTRAL SCHOOL DISTRICT K-12 ... (2017, June). Retrieved from https://www.pobschools.org/cms/lib/NY01001456/Centricity/Domain/45/K-12_Educational_Technology_Curric_Ref_Guide.pdf

Press, G. (2017, July 18). 6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry. Retrieved from https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#591b9ed5420a

Project Lead the Way. (n.d.). Retrieved from https://www.pltw.org/

RI CS Education Standards. (2018, April). Retrieved from https://www.cs4ri.org/standards

Robertson, A. (2018, September 28). California just became the first state with an Internet of Things cybersecurity law. Retrieved from https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law

Roselle Public Schools. (2018). Retrieved from https://www.roselleschools.org/departments/curriculum_and_instruction/technology_curriculum

Saluja, S., Bansal, D., & Saluja, S. (2012). Cyber Safety Education in High Schools. *International Conference on Computer Technology and Science*.

Scarsdale Public Schools / Overview. (n.d.). Retrieved from https://www.scarsdaleschools.k12.ny.us/

Science, Technology, and Engineering. (2011). Retrieved from http://www.muscatine.k12.ia.us/departments/curriculum-and-instruction/

South Carolina Computer Science and Digital Literacy Standards. (2017). Retrieved from https://ed.sc.gov/scdoe/assets/File/instruction/standards/Computer Science/FINAL_South_Carolina_Computer_Science_and_Digital_Literacy_Standards_(SBEApproved050917)063017.pdf

South Dakota K-12 Educational Educational Technology Standards. (2015, May). Retrieved from https://doe.sd.gov/ContentStandards/documents/BoardApprovededtechstandardsforweb.pdf

STEMpack: Cyber Security. (n.d.). Retrieved from https://www.aauw.org/what-we-do/stem-education/stempack-cyber-security/

Symantec. (2019). 2019 Internet Security Threat Report. Retrieved from https://resource.elq.symantec.com/LP=6819?inid=symc_symc-home-page_ghp_to_leadgen_form_LP-6819_ISTR-2019-report-main&cid=70138000001Qv0PAAS

Tate, E. (2019, February 11). Report: A New Cybersecurity Incident Strikes K-12 Schools Nearly Every Three Days - EdSurge News. Retrieved from https://www.edsurge.com/news/2019-02-07-report-a-new-cybersecurity-incident-strikes-k-12-schools-nearly-every-three-days

Technology Curriculum. (n.d.). Retrieved from http://www.bccu2.org/technology-curriculum.html

Technology Curriculum Guides / Elementary Technology Teachers. (2016). Retrieved from https://www.knoxschools.org/domain/4669

Technology Curriculum K-8 - Camden City School District. (n.d.). Retrieved from http://camdencity.ss12.sharpschool.com/divisions/division_of_school_support/curriculum/k-8_curriculum/technology_curriculum_k-8

Ten 7 Interactive, L. (2012). Online Smart, Online Safe. Retrieved from https://www.bloomington.k12.mn.us/node/221820

N. (2011, May). The State of K-12 Cyberethics, Cybersafety and Cybersecurity Curriculum in the United States. Retrieved from staysafeonline.org

Trenton Public Schools Technological Literacy. (2013). Retrieved from http://www.trentonk12.org/TechnologyCurriculum.aspx

# APPENDICES

**APPENDIX A:** Cyber Education Program Content Evaluation Coding Checklist

**APPENDIX B:** Computer Hygiene Figures

**APPENDIX C:** Computer Ethics Figures

**APPENDIX D:** Technological Skills Figures

**APPENDIX E:** Total Cybersecurity Figures

**APPENDIX F:** Correlations Figures

# APPENDIX A

## CYBER EDUCATION PROGRAM CONTENT EVALUATION CHECKLIST

Case Number:

Part A: Demographics

A1. Where is the program located? (City, State, Country)

_____

A2. What is the Social Economic Status of this location?

_____

A3. What is the gender of the school?

( ) Male

( ) Female

( ) Coed

A4. What is the size of the school?

_____

A5. Is this program:

( ) school owned

( ) corporation sponsored

( ) other

A6. What category does the program fall into?

( ) School curriculum

( ) Summer Camp

( ) University Program

( ) After School Program

( ) Conference

( ) Online

A7. How long is the duration of the program?

( ) 1 day

( ) 1 week

( ) 1 month

( ) 1 year

( ) All years attending school

( ) Other (Please Specify): _____

**A8. Who are the target participants in this program?**

**( ) Children in K-12 school programs**

**( ) Children in a specific grade (Specify which): _____**

**( ) School staff members**

**( ) School staff members/ Instruction Only**

**( ) Parents of school-aged children**

A9. What year/ month did the program initially begin?

____ /_____

A10. Is this program mandatory?

( ) Yes

( ) No

A11. Who is in charge of facilitating this program?

( ) School Teachers

( ) Specialized IT staff

( ) School Administrators

( ) College Professors

( ) Online Resource

A13. What resources are needed to facilitate this program?

( ) Computer / Lab Access

( ) Online Access

( ) Software Installation

( ) Computer Specialists/ Instructors majored in relevant disciplines

Part B: Computer Hygiene

B1. This program covers: (select all that apply)

( ) The importance of updating antivirus software

( ) How to install antivirus software

( ) How to create and maintain strong passwords

( ) Malware protection

( ) Firewalls

( ) Social media use

( ) Cybersecurity monitoring

( ) Site Credibility

( ) Cyber Incident reporting

( ) Cleaning up web history

( ) Cookies

B2. How is the topic of computer hygiene taught in this program?

( ) Lecture

( ) Online resource

( ) Handout

( ) Discussion

B3. Who is in charge of teaching computer hygiene to staff/ students?

( ) School Teacher

( ) School Administration

( ) IT staff

( ) Field Specialists

( ) Student Handbook without instructor

Part C: Computer Ethics

C1. This program covers: (select all that apply) Yes (1) No (0)

( ) Copyright laws

( ) Downloading materials from the web

( ) Hacking

( ) Computer/Cyber Laws

( ) Cyberbullying

( ) Responsible Use Policies

( ) Darknet

C2. How is the topic of cyber ethics taught in this program?

( ) Lecture

( ) Online resource

( ) Handout/ Exercise/ Case Study, etc

( ) Discussion

C3. Who is in charge of teaching cyber ethics to staff/ students?

( ) School Teacher

( ) School Administration

( ) Student Handbook

( ) IT staff

( ) Field Specialist

Part D: Technological Skills

D1. This program covers: (select all that apply)

( ) Coding basics

( ) Operating Systems basics

( ) Information Technology

( ) Networking

( ) Encryption

( ) Digital Forensics

( ) Cryptography

( ) Database usage

( ) Penetration Testing

( ) Search Engine usage

( ) Cryptocurrency

( ) Computer parts

( ) Keyboarding

( ) Word Processing

( ) Multimedia

D2. What coding languages are taught in this program?

( ) Python

( ) Java

( ) Javascript

( ) C++

( ) Scratch

( ) HTML

D3. What operating system(s) are covered in this program?

( ) Windows

( ) MacOS

( ) Linux

D4. How is the topic of technological skills taught in this program?

( ) Lecture

( ) Online resource

( ) Handout/ Lab Exercise

( ) Discussion

D5. Who is in charge of teaching technological skills to staff/ students?

( ) School Teacher

( ) School Administration

( ) Student Handbook

( ) IT staff

( ) Field Specialists

# APPENDIX B

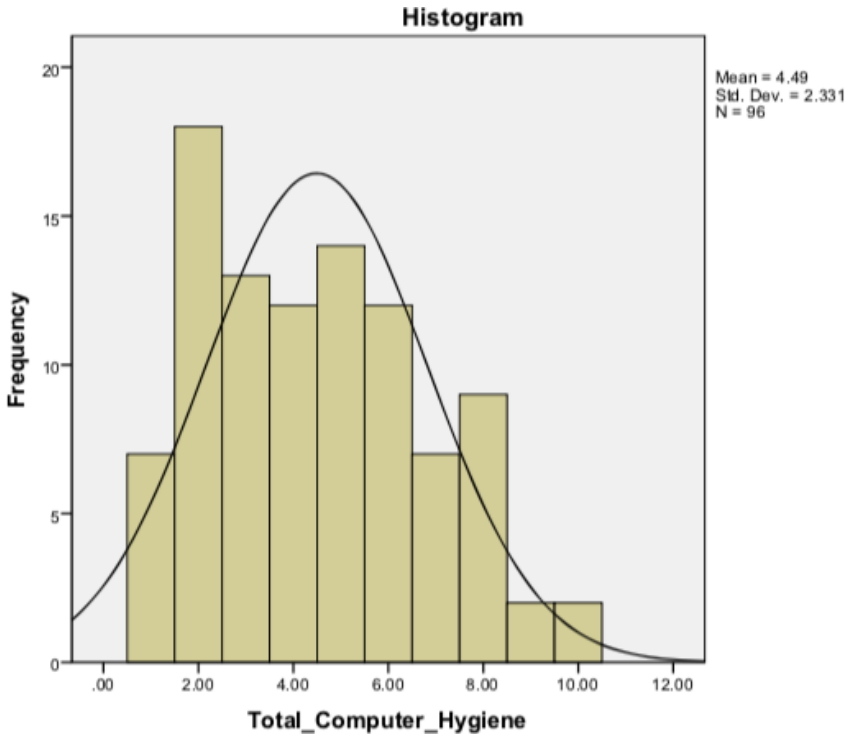
## COMPUTER HYGIENE FIGURES

FIG. 1. TOTAL COMPUTER HYGIENE STATISTICS

Total_Computer_Hygiene

| | | |
|---|---|---|
| N | Valid | 96 |
| | Missing | 0 |
| Mean | | 4.4896 |
| Std. Error of Mean | | .23786 |
| Median | | 4.0000 |
| Mode | | 2.00 |
| Std. Deviation | | 2.33055 |
| Variance | | 5.431 |
| Skewness | | .375 |
| Std. Error of Skewness | | .246 |
| Kurtosis | | -.750 |
| Std. Error of Kurtosis | | .488 |
| Range | | 9.00 |
| Minimum | | 1.00 |
| Maximum | | 10.00 |
| Sum | | 431.00 |
| Percentiles | 80 | 7.0000 |

FIG. 2. TOTAL COMPUTER HYGIENE HISTOGRAM



# APPENDIX C

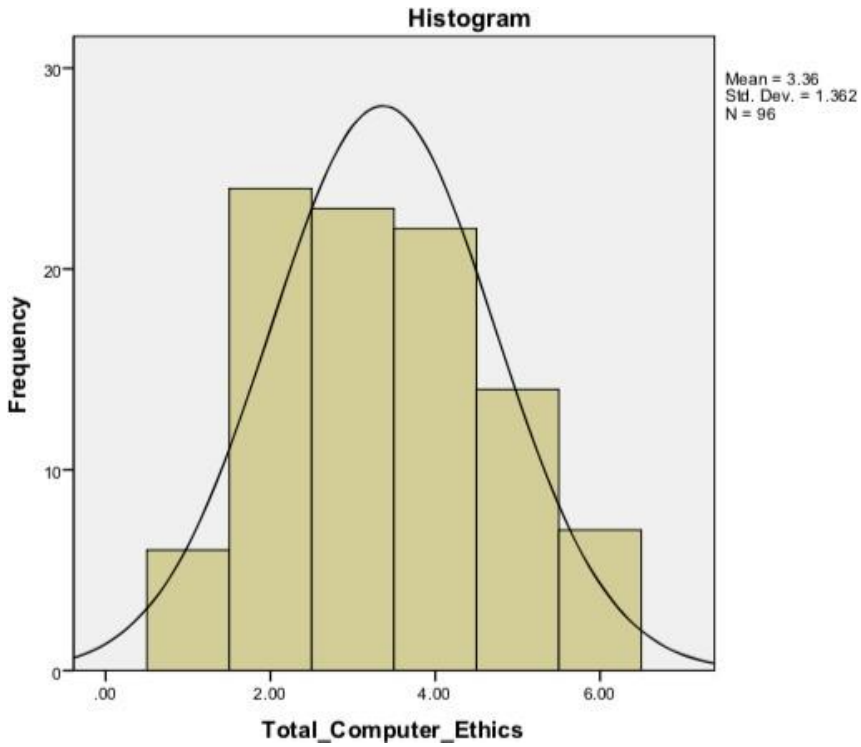
## COMPUTER ETHICS FIGURES

FIG. 1. TOTAL COMPUTER ETHICS STATISTICS

Total_Computer_Ethics

| | | |
|---|---|---|
| N | Valid | 96 |
| | Missing | 0 |
| Mean | | 3.3646 |
| Std. Error of Mean | | .13901 |
| Median | | 3.0000 |
| Mode | | 2.00 |
| Std. Deviation | | 1.36204 |
| Variance | | 1.855 |
| Skewness | | .228 |
| Std. Error of Skewness | | .246 |
| Kurtosis | | -.775 |
| Std. Error of Kurtosis | | .488 |
| Range | | 5.00 |
| Minimum | | 1.00 |
| Maximum | | 6.00 |
| Sum | | 323.00 |
| Percentiles | 80 | 5.0000 |

FIG. 2. TOTAL COMPUTER ETHICS HISTOGRAM



# APPENDIX D

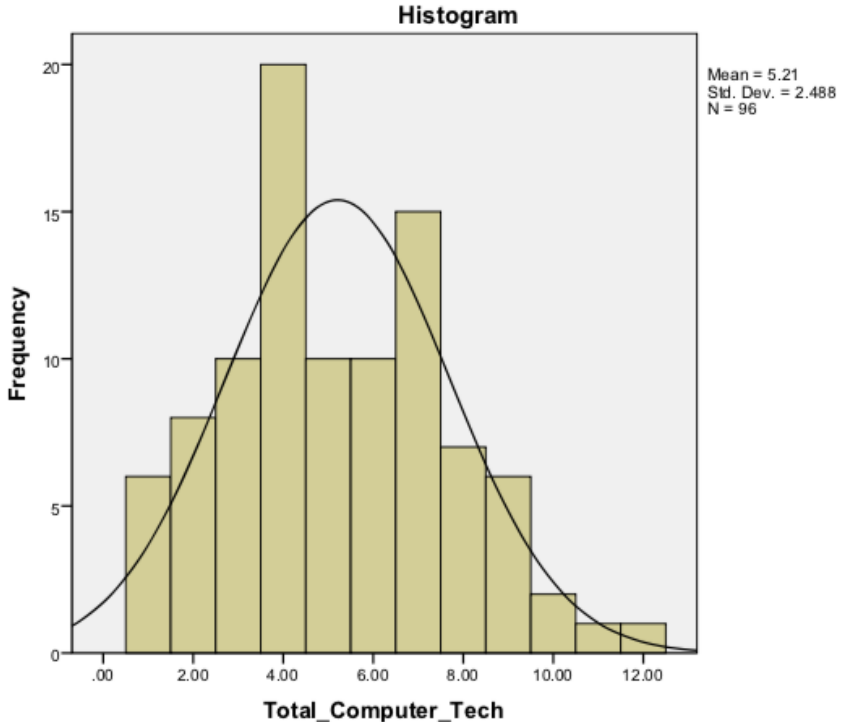
## TECHNOLOGICAL SKILLS FIGURES

FIG. 1. TOTAL TECHNOLOGICAL SKILLS STATISTICS

Total_Computer_Tech

| | | |
|---|---|---|
| N | Valid | 96 |
| | Missing | 0 |
| Mean | | 5.2083 |
| Std. Error of Mean | | .25388 |
| Median | | 5.0000 |
| Mode | | 4.00 |
| Std. Deviation | | 2.48751 |
| Variance | | 6.188 |
| Skewness | | .310 |
| Std. Error of Skewness | | .246 |
| Kurtosis | | -.420 |
| Std. Error of Kurtosis | | .488 |
| Range | | 11.00 |
| Minimum | | 1.00 |
| Maximum | | 12.00 |
| Sum | | 500.00 |
| Percentiles | 80 | 7.0000 |

FIG. 2. TOTAL TECHNOLOGICAL SKILLS HISTOGRAM



# APPENDIX E

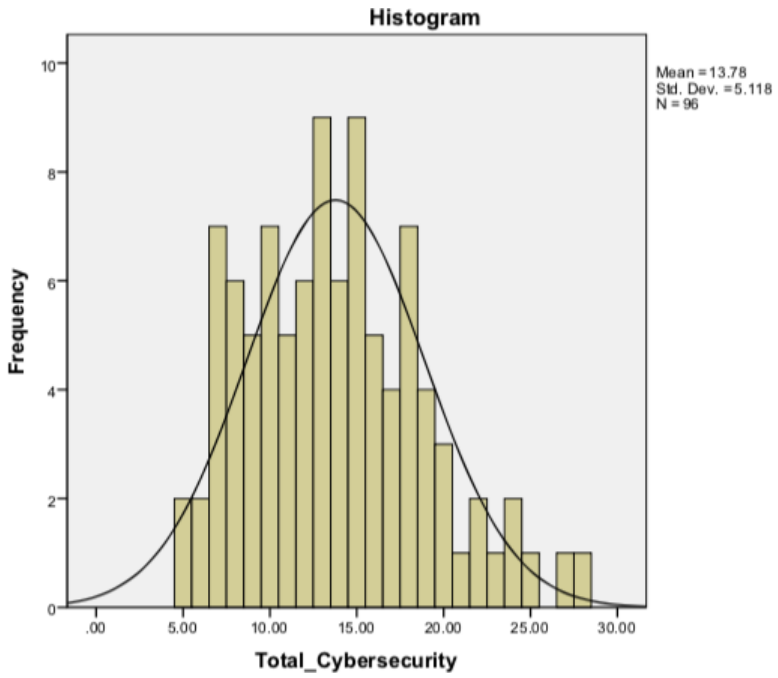
## TOTAL CYBERSECURITY FIGURES

FIG. 1. TOTAL CYBERSECURITY STATISTICS

Total_Cybersecurity

| | | |
|---|---|---|
| N | Valid | 96 |
| | Missing | 0 |
| Mean | | 13.7813 |
| Std. Error of Mean | | .52235 |
| Median | | 13.0000 |
| Mode | | 13.00[a] |
| Std. Deviation | | 5.11798 |
| Variance | | 26.194 |
| Skewness | | .506 |
| Std. Error of Skewness | | .246 |
| Kurtosis | | -.098 |
| Std. Error of Kurtosis | | .488 |
| Range | | 23.00 |
| Minimum | | 5.00 |
| Maximum | | 28.00 |
| Sum | | 1323.00 |
| Percentiles | 80 | 18.0000 |

FIG. 2. TOTAL CYBERSECURITY HISTOGRAM



# APPENDIX F

## CORRELATIONS FIGURES

FIG. 1. MANDATORY TO PROGRAM OWNERSHIP CHI-SQUARE CORRELATION STATISTICS

**Chi-Square Tests**

| | Value | df | Asymp. Sig. (2-sided) |
|---|---|---|---|
| Pearson Chi-Square | 73.181[a] | 3 | .000 |
| Likelihood Ratio | 68.285 | 3 | .000 |
| Linear-by-Linear Association | 24.922 | 1 | .000 |
| N of Valid Cases | 96 | | |

FIG. 2. MANDATORY TO PROGRAM OWNERSHIP CHI-SQUARE CORRELATION BAR GRAPH

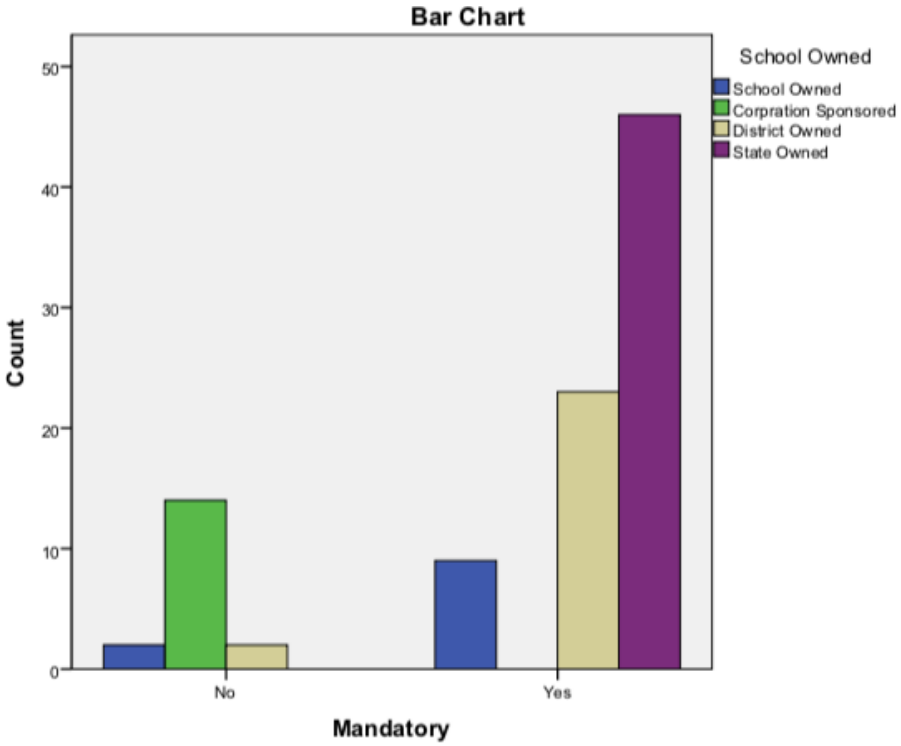


FIG. 3. DURATION TO EFFECTIVENESS SIGNIFICANCE STATISTICS

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 196.320 | 355.199 | | .553 | .585 |
| | Duration of the program | 2.949 | .948 | .510 | 3.110 | .004 |
| | StartDate | -.101 | .177 | -.092 | -.569 | .574 |
| | Mandatory | -1.229 | 1.673 | -.118 | -.735 | .468 |

FIG. 4. METHOD TO EFFECTIVENESS SIGNIFICANCE STATISTICS

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 2.674 | .606 | | 4.411 | .000 |
| | Handout/ Lab Exercise | 1.981 | .500 | .374 | 3.960 | .000 |
| | Discussion | 1.414 | .644 | .207 | 2.194 | .031 |

FIG. 5. INSTRUCTOR TO EFFECTIVENESS SIGNIFICANCE STATISTICS

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 2.309 | .850 | | 2.716 | .008 |
| | School Teacher | 2.012 | .809 | .237 | 2.486 | .015 |
| | IT Staff | 2.402 | .474 | .483 | 5.065 | .000 |