HIGH SCHOOL EDITION
Journal of Student Research
Volume 10 Issue 1 (2021)

Cybersecurity of The Future Nevadans

Omid Najibzadeh[1] and Soo Park[1]

[1]Advanced Technologies Academy, Las Vegas, NV, USA

ABSTRACT

With the increased level of digitization, the role of cybersecurity has been at the forefront of security discussion. However, the literature displays a lack of proper knowledge and preparation in everyday individuals. This study examined the potential need for and implementation of cybersecurity education in CCSD. The results indicated interest within students and an advocation by cybersecurity experts. This study concludes and advises for an awareness training campaign, especially a real-life treat simulation.

Introduction

Equifax ©, Marriott ©, Target © are few famous companies among the lengthy list of the decade's groundbreaking cyberattacks. In the past two years alone, there have been over two hundred government orientated or targeted cyber-attacks (CSIS, 2019). With the spread of technological advancement and computer dependence, cyber involvement has risen dramatically; however, security has fallen short. In fact, 43% of Americans have experienced some sort of cyber-attack at some point (Smith, 2017). This trend will most likely grow with future generations —due to the rising digitalization. To prepare the future for the cyber world, policymakers and company executives have devoted resources to developing future cyber-prepared individuals. From 2013 to 2018, the number of states with at least one computer policy raised from 15 states to almost the entire country (Code.org, 2018). However, the majority of these policies involve computer literacy and/or coding. Being able to use a computer does not equate to cyber preparedness. Technology or IT is an overarching umbrella that encompasses a plethora of specialized fields. In the same way that apples and oranges are both fruits, yet they are completely different, cybersecurity and computer science share an identical comparison.

Therefore, one's standards cannot cover the other's knowledge. Cybersecurity—as defined by the Cybersecurity & Infrastructure Security Agency (the overarching body in charge of protection and preparedness against cyber-attacks and exploits) as the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information (2020). Any type of online policy ranging from simply setting a password to complex algorithmic protocols lies beneath the umbrella of cybersecurity. With such an extensive range, this umbrella encompasses both personal security and enterprise security. As stated previously, most notable of the cyberattacks fall under the business aspect; however, this does not dictate the personal aspect does not carry substantial worth. While business attacks have more reaching effects, an individualized attack or exploit may have everlasting consequences for that individual—far more than any business attacks. To combat this problem, businesses hire cybersecurity specialists and buy expensive equipment such as firewalls, filters, etc. Individuals, on the other hand, barely act upon this problem despite its possible consequences because of the lack of resources, awareness, and capabilities. This leads to the current problem regarding cybersecurity: unaware individuals are helpless against potential hackers. Therefore, it is safe to assume that cybersecurity knowledge is a powerful and essential tool for most adults in the modern age because without such information the individuals could suffer severe consequences. Due to cyber knowledge's extensive value, the question arises whether secondary education facilities should add content to their program. To do that, first, the students' current capability must be measured. A thorough examination of the literature illustrates that the majority of high school graduates today lack the capabilities to protect

themselves against cyber threats. A significant finding in this field was the result of a study conducted by the University of Albany's researchers led by Zheng Yan (2018). In their study, they examined 462 college students ' cybersecurity judgment. They found that the students were correct 65 percent of the time; however, this percentage was equal to the institutional judgment suggesting that college students lack extensive cybersecurity thinking ability—which can be costly if they were to be targeted (Yan, 2018). This study serves as proof to the extent of the cybersecurity dilemma for the upcoming generation. This study simply looked at the logical processing, which does not include any particular cybersecurity-specific information. Logical processing is only a necessary mindset that an individual must possess to notice and strategically combat a cyber crisis—only the mindset. On the other side of the world, Bartın University of Turkey (2017) conducted a similar study, revealing the same results: they found that secondary students are also at risk online because of their insufficient understanding and education (Yılmaz).

The parallel between the studies demonstrates the new interconnectivity in the cyber world. Today, a hacker from Russia can target a Nigerian businessman, for instance. Cybersecurity is not just a state problem, it's worldwide. This can range globally all the way down to a personal file on the family's computer; without proper protection, when students become adults, their lives are at serious risk; as stated by conclusion by Bartin University: lack of education was the primary reason for such frightening results. As a proud resident of Southern Nevada, the topic of cybersecurity training in education is examined. As stated in Clark County School District(CCSD) mission statement, the purpose of the school is "[to] prepared to succeed and contribute in a diverse global society". Under the mission's umbrella, preparedness for a future occupation will be an essential key to "success" and "contribute". This leads to the second incentive for schools to adapt to such curriculum: cybersecurity career. Today, cybersecurity jobs are one of the highest-paid due to demand in the job market. Because of this, a variety of high school and college cyber platforms appear to propel students for a cybersecurity career. A perfect example of such a program is Air Force Cyberpatriot. As stated in their mission statement, Cyberpatriot is a program created to "inspire K-12 students toward careers in cybersecurity." At the federal level, the executive office has provided "$15 billion of budget authority for cybersecurity-related activities." according to the FY 2019 President's Budget.

This incentive has led to many schools adding a cyber program or classes. For example, in CCSD alone, there will be over ten new schools with a cybersecurity program starting in 2020. Although these programs are meant as pathways to a cybersecurity career, they also prepare students for the cyber world, therefore, they are considered a preparation tool as well. In other words, in the pursuit of a cybersecurity job, students will become ready for the real-world cyber threats or will be influenced towards a career in the cybersecurity job. The two reasons (need for individual cybersecurity training and potential jobs) have many different institutions implementing different approaches to teach cybersecurity material. In order to answer the initial question on whether schools should adopt cybersecurity education because of two stated incentives, a subsequent question arises: should schools in CCSD adopt cybersecurity education and how? To determine the best possible solution, the previous research and solutions must be analyzed and introduced.

One solution proposed was the implementation of cybersecurity standards into the business curriculum. Such a solution is sensible since business employees are the favorite target for corporate hackers (Weiser/BizEd). However, such a solution only targets a small demographic and is not yet proven to be effective. In addition, another problem with any solution is that any hacker's strategy involves locating vulnerability and exploiting it. Strengthening one area does not guarantee total protection- it will only shift the problem. Also, this solution will also be only realistically applied in college since not many high schools have any business classes.

Following the same strategy, the research from the University of Florida conducted by Michael Berson, implemented the cybersecurity concept in the social studies department. Since social studies is required for all high schools and colleges- this can spread to all students- unlike the business class model. However, the degree to which this cybersecurity can be thought will be significantly lowered since it will most likely be only a unit or two. Not to mention, the change of standards will be controversial since cybersecurity must replace an existing standard. Next, teachers will have to be trained- requiring a variety of hurdles and obstacles. On the other side, simply introducing the topic and its history can provide noticeable insight for students.

In another study by California State University, San Bernardino's Joon Son, the implementation of virtual labs was tested. In their findings, they concluded that virtualization provides a substantial and effective real-world experience. This tool could be implemented across the United States, with the proper resources, to provide real-life scenarios for students to learn from, and it has already begun. Cyberpatriot uses virtual machines in student's schools to run its competition, reducing a significant cost from both themselves and the schools and competitors.

Through a social representation lens looked up a survey of 153 University students and found that through a social representations map students' motivation can be advanced and nourished. This study goes as far as to claim that the social associations of cybersecurity is can have implications regarding students interests in cybersecurity. So, for the purposes of this research the stigma of cybersecurity will accounted for a limitation that yet needs to be addressed.

Looking outside the school, Dr. Yin Pan of Rochester Institute of Technology looked towards a fun way to prepare students for the cybersecurity-through games. He and his colleagues came up with critical thinking games to allow for fast entry to the cybersecurity path. These games were designed for only entry level students. This way the student can see cybersecurity as what it really is: a critical thinking activity. The simplicity of the games allows for the critical thinking to develop without putting confusing the student. This strategy is simple and cost effective. However, further studies are required to see whether the claims made by Dr. Pan can hold true in the real world and the cyber careers.

Through the discussion of the literature, it is clear that there are multiple relatively effective solutions to draw upon for any entity. However, a key aspect that has not been addressed by any of the research papers is the students' preferences and overall view of these implementations. As a matter of fact, the students have not contributed or provided any feedback for the questions at hand. After all, playing to students' interests in the content that they are learning is essential in a strong learning environment and leads to higher levels of learning and engagement for the students (Harackiewicz, Smith, Priniski). Yet, most of the literature fails to consider this factor into consideration and the ones that do so are non-generalizable due to the nature of the factor—since the variability is extremely high from location to location. Next, expert cybersecurity opinions are also lacking in the research that was studied for the purposes of this study, and the ones that did consider expert opinion are outdated due the nature of ongoing changes in the cyber/technological world. With that stated, in order to answer the essential question of this study, those two factors must be addressed; therefore, this study will focus on this gap, leading to focus towards polling CCSD students' interests and views towards cybersecurity and acquiring expert opinion regarding the establishment and implementation of cybersecurity curriculum into CCSD standards or Nevada's department of education's standards, allowing for a new and more defined understanding of the issue and its plausible solutions.

Methodology

In order to get a better understanding for the upcoming cybersecurity threats regarding future Nevadans, a mix method study was conducted, examining high school students' current views and potential interest in different strategies of execution of a cybersecurity education and evaluating those strategies with current top information security (cybersecurity) experts. For sake of simplicity this is divided into two elements: quantitative element and qualitative element, in that chronological order— since the students' interest was the frontrunner solution, it was key that information was collected before the expert evaluation.

Element I - Quantitative Survey

A survey methodology was implemented in this study to provide a suitable access for students to give their insight. A survey is the most tailored instrument since it allows for easy access for students. In addition, students felt less pressure and were able to express themselves and their interests. The study included two different sets: one with close ended questions and other with open-ended. The survey was sent to all schools in CCSD, however, schools with

cybersecurity classes were noted to ensure objectivity— the results were differentiated based on the type of school. Next, the survey was sent electronically so that it was given to students to complete on their electronic device of their own choosing. Using Google Forms©, any student with a computer and the link can be able to submit the survey. Not all questions were required, allowing for a short time needed for completion. This will ensure that students give a higher level of effort in required questions. Student's honesty and accuracy is fundamental to a full picture regarding this new concept. Therefore, by allowing this survey to be anonymously submitted (yet limited to one per student), the students can feel secure regarding their answers and respond with full certainty. It should be noted that although all schools were given the survey, only a handful accepted to distribute it, majorly due to time and convenience.

From there, one instructor from the school provided the link to students and allowed time to finish the survey in class. The process was not mandatory for any student and students had the right to quit in the middle of the survey without anyone knowing nor any consequences. Since the expected participation for the survey was predicted to be high compared to the total number of high school students in the district, the entire respondent sample was used, unless an abnormality was detected: putting the first answer for everything, despite contradicting oneself. Fortunately, none was detected. Most importantly, to ensure that only qualified individuals were able to take the survey, individuals must have sign-on with their CCSD Google accounts to be able to take the survey. The survey itself was delivered on the week of December 4th, 2020. The survey remained open for the entire week, up to 11:59 of local time.

This time frame was chosen so that students do not get influenced by semester exams or "end of school rush", while ensuring that students and school has been stabilized with their schedules and teaching plans; therefore, students were most likely comfortable and familiar with the classroom, allowing them to share their ideas freely. On to the survey itself. The survey titled was clearly present at the top of the page as: Cybersecurity/IT Survey Interests Student Form. Next, in the description sections, a detailed purpose statement of the study was shown alongside potential entities that might have access to the results. Next, multiple types of questions were asked, starting with a yes and no question asking whether a student has any previous IT background (this has been done to eliminate any potential biases). Next, multiple questions are asked in a form that students are to choose from a scale to show their exact degree of answer. These questions were later used for multivariable analysis to see the influence of individuals' view towards cybersecurity, more specifically online safety for students' case. The answers for those answer the question if pattern exists between the feeling of cybersecurity for the student and their interest levels- which could lead to different interpretation of the results, since as stated previously, statistically most students do not capability to correctly protect themselves in the cyber world. After, a list type question is asked, asking the student to choose any of the following types of cybersecurity education. Finally, the students are allowed to add any comments or suggestions in a box. For exact details on the questions and its presentation please see figure 1 and figure 2 (a replicate Google form link is also available below exhibit A and B for any replication purposes and hereby under the public domain).

Figure 1:

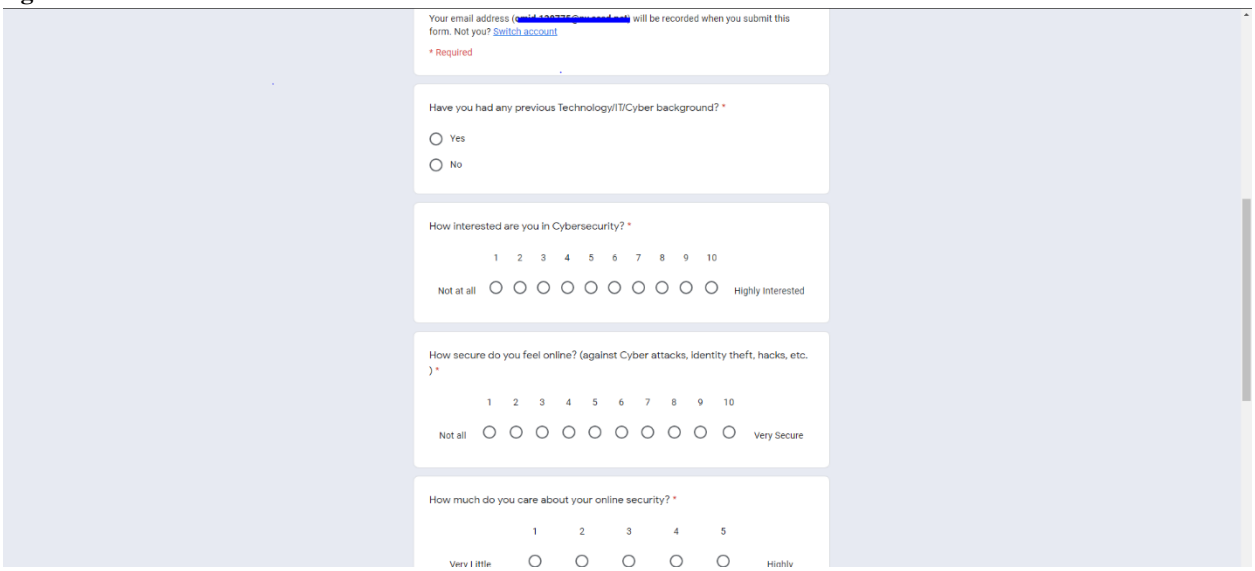
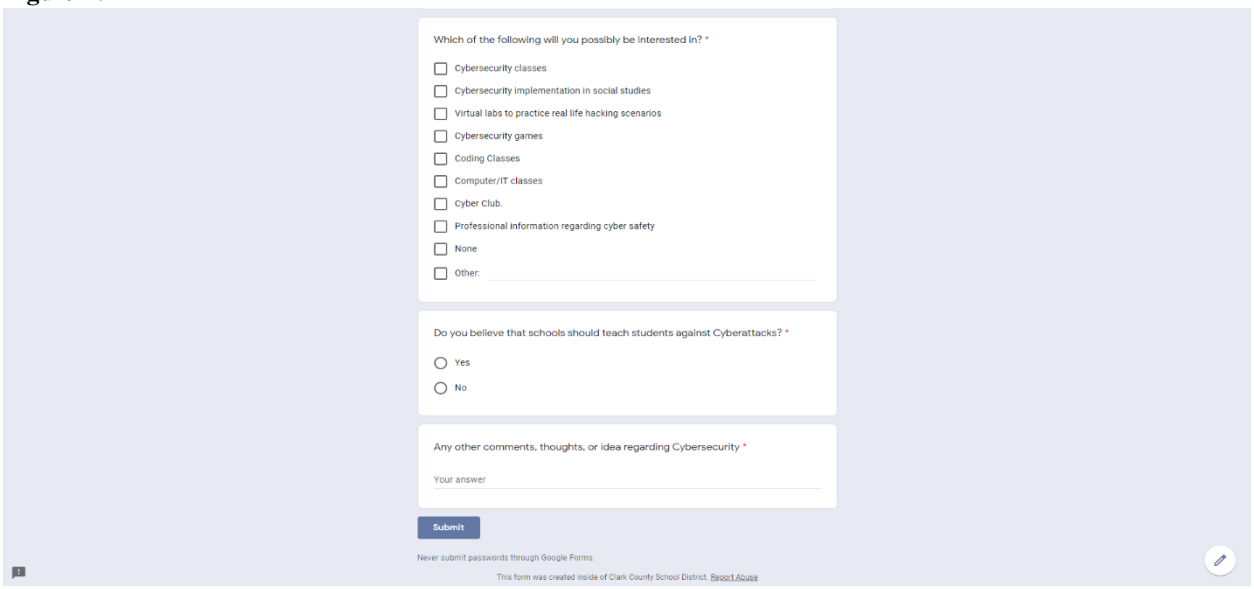


Figure 2:



Element II - Qualitative Interview with Information Security Experts

For element II, this study encompassed a semi-structured interview system to best capture the desired information. This system allows for topic focused discussions while allowing the experts to add and guide the conversation towards a subtopic that could be potentially best suited for the discussion. Furthermore, this structure provides flexibility so that potential new solutions could be discussed and would not be restricted by the structure of the interview. To ensure that the interview best utilizes the expert's time and resources, the interview was designed for the expert's role and expertise; therefore, the interviewee was asked different questions on multiple topics.

Interview with Carl Agbayani: Director of Information Security of Switch Inc.

As stated previously, each expert will have a tailored interview. As the Director of Information Security, Director Agbayani is responsible for managing data center operation, investigating potential anomalies, and looking out for any potential exploits. With his advanced experience in military and penetration testing, he is well equipped with hacking strategies and defense mechanisms. For that reason, his interview was divided into four categories: 1) Big Picture, 2) Individual Security, 3) Southern Nevada's cyber community and resources, 4) Cybersecurity careers. The purpose of each of the categories is as follows:

Big Picture

The world of technology is forever changing and keeping up with best practices is critical to any cybersecurity research and execution. Knowing the current trend of the field and potential upcoming technologies or guidelines is detrimental. In this category, Director Agbayani had a chance to discuss how he perceives what cybersecurity is and how he expects it to change.

Individual Security

The main topic of this research is to explore solutions to better help individuals protect themselves from cyber exploits. This category targets that focus by allowing Director Agbayani to illustrate what he considered is best practice for individuals and what he does personally. This section allows for expansion of previously known solutions and add or subtract potential standards that should be included in cybersecurity education.

Southern Nevada's cyber community and resources

In this category, the exploration of local resources available to the state and local educational institutions is discussed. Especially with countless government and privately funded cybersecurity institutions trying to promote awareness, this research deemed the investigation of the resources available to maximize a solution necessary.

Cybersecurity Careers

The second incentive for schools to implement solutions is future job preparedness. This category looks deeper regarding potential jobs in cybersecurity and the future outlook for those jobs.

Interview with Dr. Arthur Salmon.

Dr. Salmon is the director of cybersecurity at College of Southern Nevada, and professor at Liberty University. He has helped create Nevada Department of Education's cybersecurity curriculum (for the cybersecurity program—high school major) and has volunteered as a guest instructor for many high school cyber competitions. In his professional career, he has been a consultant for many top companies and currently has his own information security company, providing security services and operations. Finally, he possesses a wide range of professional certifications ranging from Certified Ethical Hacker to Cisco Certified Design Professional. In his interview the topics of discussion were divided into three main categories:

Cybersecurity Risk in Southern Nevada

This topic embraces the specific treats that are unique and most prevalent for residents of Southern Nevada.

CCSD breach and current cybersecurity regulations and executions.

A continuation of the previous topic, explaining how the user's protections under the law, and potential need for cybersecurity awareness.

Potential Implementations and solutions to CCSD cybersecurity training.
Analyzing potential implementation and asking for his professional opinion on a solution for teaching accurate and effective cybersecurity information.

Results and Analysis

Element: Quantitative Survey

The survey received exactly 110 respondents from 3 different public high schools within CCSD. The respondents' email, after confirmation of their enrollment within CCSD plus their high school status, was removed. Before any analysis, an abnormality check was conducted looking for clicking the first response on all questions despite contradiction: None was detected. Initially, the difference between students' with and without background in IT and cybersecurity was analyzed to see if the experienced population might skew the results of the overall study.

Table 1: Students with IT background

	How interested are you in Cybersecurity?	How Secure do you feel online?	How much do you care about online security?
Valid	28	28	27
Missing	0	0	1
Mean	6.286	7.143	4.444
Median	6.500	7.000	5.000
Mode	7.000	5.000	5.000
Mode St. Deviation	2.275	2.013	0.641
Variance	5.175	4.053	0.410
Range	8.000	7.000	2.000

Table 2: Students without IT background

	How interested are you in Cybersecurity?	How Secure do you feel online?	How much do you care about online security?
Valid	83	83	83
Missing	0	0	0
Mean	4.928	6.542	4.108

Median	5.000	7.000	4.000
Mode	5.000	5.000	5.000
Mode St. Deviation	2.443	2.143	1.104
Variance	5.970	4.593	1.220
Range	9.000	9.000	4.000

As seen in table 1 and table 2, a noticeable difference is seen in both mean and median of the following questions regarding interests and safety levels. This led to the decision to only use students' with no background since that is assumed to be the supermajority of the CCSD students, and most likely the most vulnerable population of the students; however, a small discussion regarding the differences between them was considered for future research purposes.

The first noticeable figure in the data is the interest level of student for cybersecurity(see table 2): from a scale of 1 to 10 the mean is a 4.9 and the distribution is comparable to a normal distribution centered at 5. Since 5 is a neutral answer this could explain why the mode is at 5; therefore, skewing the data slightly. Overall, it seems that "a neutral" interest exists for cybersecurity where some students would be likely to contribute a substantial amount of time while others likely do not want to participate. What is clear however, is that an overwhelming majority of the students care regarding their online safety as displayed by table 2. From a scale of 5, the mean of approximately 4 is a strong indication of students' desire to stay safe. There could be a remaining wording effect in this study where students might not be aware of cybersecurity's role in online safety and how they intertwine. Arguably, many might be interested in the personal concepts of cybersecurity but might receive the wrong ideas regarding what cybersecurity means. With all that said, it is also clear how students would like cybersecurity thought in schools—about 80% of students responded that schools should teach cybersecurity. Students were also asked if they were interested in some of the potential solutions outlined in the literature review. From the without background students, all the students' responses are represented in table 3. From a sample of 83 non-tech background students only 6 students (not the same students for each option) responded interest in virtualization labs, coding classes, and cybersecurity classes.

Table 3: Without Background IT Students

Which of the Following will you possibly be interested be in?	Number of responses(descending based on popularity)
None	21
Virtual labs to practice real life hacking scenarios, Cybersecurity	6
Cybersecurity games, Coding classes	5
Cybersecurity games	4
Virtual labs to practice real life hacking scenarios, Cybersecurity games, coding classes	4
Coding classes	3
Cybersecurity classes	3
Cybersecurity classes, Virtual labs to practice real life hacking scenarios, Coding classes	3
Cybersecurity classes, Coding classes	2
Virtual labs to practice cybersecurity classes, Coding classes	2

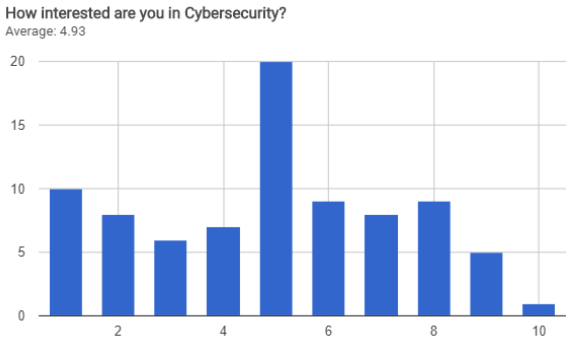
Virtual labs to practice real life hacking scenarios, Professional information regarding cyber safety	2

*Not all results are shown

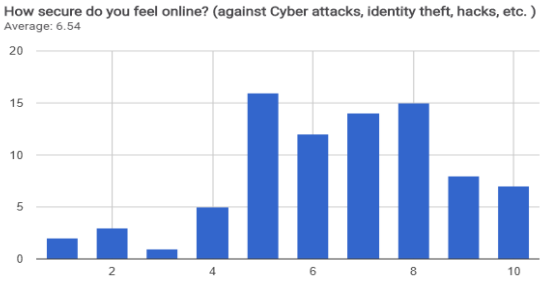
Table 4: All Students	
Which of the Following will you possibly be interested be in?	Number of responses(descending based on popularity)
Coding Classes	50
Virtual labs to practice real life hacking scenarios	49
Cybersecurity games	47
Cybersecurity classes	29
Computer/IT classes	29
None	25
Professional information regarding Cybersecurity	15
Cybersecurity implementation in social studies	7
Cyber club	5

Yet almost every tech-background student (26) showed interest in all of the three activities listed. This number alone should be enough for a school to possibly start class for those students. As high as 26 is, it is far from even a majority; therefore, more consideration needs to be taken before mandating such class or classes.

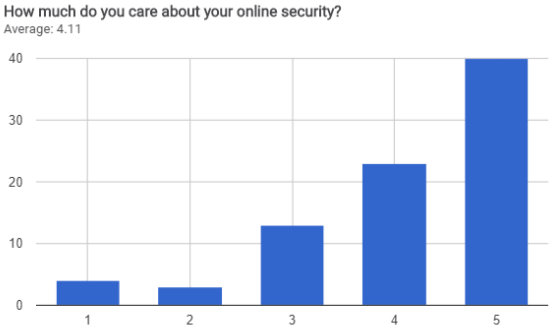
Students Without Background



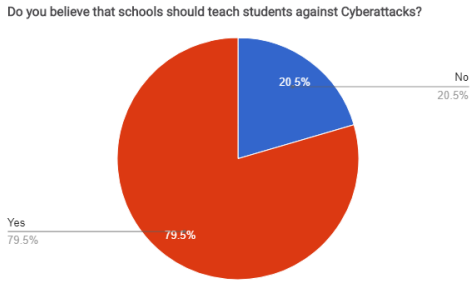
Graph 1



Graph 2:

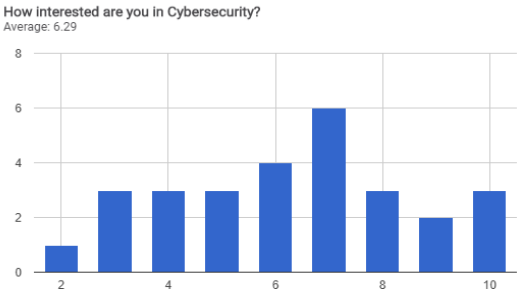


Graph 3:

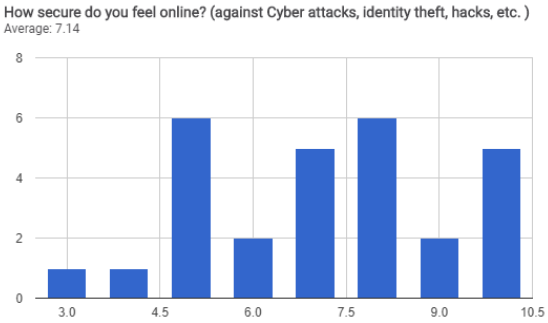


Graph 4:

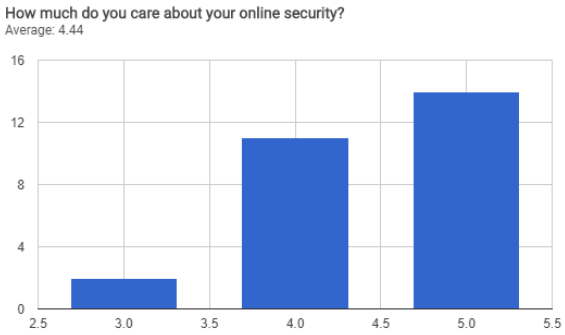
Students with Background



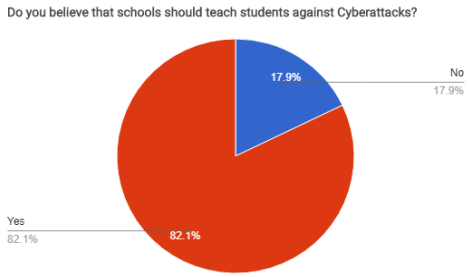
Graph 5:



Graph 6:



Graph 7:



Graph 8:

The last question, the open-ended questions, also received some fascinating responses worth looking into. Over 7 students overall said something related to hacking which goes to show how the media has influenced the view when it comes to cybersecurity since the majority of movies and TV shows portray an unrealistic picture of the reality of hacking or security (this is only a plausible reason, this study does not prove, claim or support this statement). For the full detail of the survey data please refer to table 1 through 3 and graphs 1 through 8 for a visual representation.

Element II - Qualitative Interview

Interview with Carl Agbayani: Director of Information Security of Switch Inc.

The interview with Director Agbayani turned out to have much of a familiar tone, which allowed him to share freely without too much filtering. His views and responses towards the four categories explain in Methods Element II is summarized as follows:

Big Picture

Most of his big picture analysis tied to the following sections. By one note that stood out is the way he described the change in industry. He said that companies are releasing the actual risk behind the internet and now are trying to get protected.

Individual Security

He described cybersecurity into two different categories: business and individual. He explained how individuals barely have any control over their majority of their information on the business side. The only factor that they can control is how much information leaks from them. Most notably, he described educating best practice personal cybersecurity would only take 15min for the “essentials” and a bit more time for “beneficial” information. This short time follows how little control individuals have with their information. He talked about an example of such 15-training material would include strong passwords, active awareness for potential threats, and being smart and following common sense.

Southern Nevada's cyber community and resources

Although he claimed he was aware of everything that was happening in the district in regard to cyber, he didn't discuss too much regarding cybersecurity communities. In his mind, the necessary training/education was so minimal it does not require any expert help.

Cybersecurity Careers

Regarding career, he was extremely optimistic. He said that since more and more companies are going digital, only more jobs in IT and security are going to arise. Not to mention, there is already a huge shortage in the industry. Then he went on to describe how the key is keeping with a company that respects and appreciates its cyber/IT department.

Interview with Dr. Salmon

Dr. Salmon's free discussion style of interview allowed a deep connection among the main topics of the interview. He provided his own view on the solution for CCSD and stated that he does believe in a CCSD universal cybersecurity education. The main themes are as follows:

Cybersecurity Risk in Southern Nevada

Dr. Salmon explained how phishing is among the biggest cybersecurity threat in Southern Nevada. He emphasized the role of cybersecurity planning and region-based analysis—showcasing the uniqueness of each region in terms of cybersecurity threats and needs. He stated the general public has "zero-clue" in regard to cybersecurity. The general public, as he mentioned, expect someone else to protect them. He notes that in this new age of digitalization there is a new accountability portion that society is not yet ready to accept, especially cyber individual responsibility. This leads to a gap in the level of awareness people have. To get a more exact picture, the interview led to the CCSD breach.

CCSD breach and current cybersecurity regulations and executions.

Dr Salmon explained that currently, Nevada has regulations in place for cybersecurity and accountability; however, they are not being enforced. In the case of the CCSD incident where CCSD was hacked and numerous of employee's personally identifiable information or PII was breached and leaked. Dr. Salmon criticized CCSD for their lack of transparency even though the Nevada law depicts that a public announcement regarding breaches must be made—yet CCSD's announcement was half-hearted.

Potential Implementations and solutions to CCSD cybersecurity training.

The majority of the interview revolved around Dr. Salmon's suggestion on a potential plan for CCSD. His plan involved an ongoing series of updating curriculum to best fit the changing world of cyber, claiming that each year the lessons will become outdated due to the nature of technology. Next, he explained that cybersecurity is not a 10-minute topic that can be thought, and people will understand. Simply attending a lecture is not enough. He further explained that this process is an on-going process where it must be mostly application based. A user is not going to care about a phishing attempt simply because he learned about it years in the past in a brief lecture. He suggested an ongoing training routine like how companies send their own phishing attempts to help facilitate and train them. He claimed that this must continue the entire educational cycle and it cannot be either one time or predictable. When Answering the question of when should this training regimen begin, Dr. Salmon answered that it should start as soon as anyone is using technology, claiming that this is a new cyber age and this will be part of life now. One suggestion the interviewee made based on Dr. Salmon's recommendation was a grade for cybersecurity where the student needs to pass by avoiding getting hacked: Dr. Salmon agreed. This went to show the main theme in Dr. Salmon's interview: practice and application.

Conclusion

Before any conclusion can be drawn from the data, the limitations must be assessed to fully understand the reach of validity and reliability of the claims that can be made. First, Element I conducted using a volunteer sample population rather than a random sample population; this itself could have skewed or distorted the results. Next, due to the lack of a pilot study, the extent of wording bias, availability bias, and other technical problems could not have been assessed and corrected, limiting the reliability and validity of the study. Another factor relating to the reliability of the study is its number of attempts: the survey was only given out in a single time frame; however, to the defense of the process, the purpose of the study did not require experiment level scrutiny—yet this limitation should still be considered. Last but not least, in Element II, only two expert was interviewed due to COVID-19, restricting the scope to which this study can claim that this study gathered the guidance of the expert community in cybersecurity. Note that this study only considered the case of CCSD and does not claim its results are generalizable to any other region, which some might consider another limitation.

At the beginning of the analysis, the data was separated into IT background and without background groups. This was since people with interests in IT are logically more likely to have a background, so those 28 respondents were removed from the data. From the rest of the data, an average interest level of 5 was shown, which goes to show how the students have some interests, yet barely any students showed overwhelming interests. Therefore, the solution of creating a statewide cybersecurity credit requirement becomes ill-advised since the students would not be interested enough for such a class, leading to lower learning. Not to mention, as Director Agbayani mentioned, there is only so little fundamentals needed for students to learn, meaning the rest of them will be content for the professional level cybersecurity field. This helps the case for the solution to adapting cyber education into social science departments. However, it will be extremely unlikely that teachers themselves will be equipped to be able to teach such content, and even more difficult to answer students' questions. The next option to consider will be a virtual lab. The virtual lab was a favorite in the select question and has mass implementation capabilities. Most schools have enough computing power to be able to execute a simple virtual machine, similar to how science classes use virtual labs using Java or flash. Another suggestion that was under consideration from the research team was the idea of guest speakers. This was the primary purpose behind the community section for the interview. Guests experts could come every year to talk to high schools in for example cyber awareness month (October) and go through all of the essential education in one assembly or class period. This method will only be possible if experts agree to contribute their time and effort, and not all schools might get a speaker. Thus, flexibility is key in such a strategy. Leaving it up to schools to be able to gather guest speakers, and provide resources and guidelines, like virtual lab software, from the district or even the state. If possible, schools can also start their own cyber classes. This way, they can hire professional cyber instructors that can prepare students for cyber careers and teach them about the potential cyber vulnerability—the teacher can also act as the speaker for other students to provide them with the basic essential training as well(again a training that should take “15min”). To ensure accountability, districts can act as a self-report system where schools report how they have helped train students and districts can later guide and help struggling schools. Again, if possible, the district could hire a penetration tester to try to hack schools randomly to show a real-life example, making it more fun for students as well.

With all of the solutions and this research’s implications on the solutions, the suggested plan is a combination of Dr. Salmon’s approach and the guest speaker’s approach. First, as Dr. Salmon explained, the preparedness must start early, even as soon as elementary school or even earlier. For the scope of this research, only secondary education is focused upon. Second, it is important to teach students with regard to the potential threats facing them. For example, students need to know that hackers use emails as a primary way of getting access to credentials unlike what they see in movies. Therefore, schools should have the option to choose their own method of teaching the theory. However, when it comes to practice, Dr. Salmon’s approach leaves little ambiguity. Unlike a class, students should be provided training, similar incorporation, where they are tempted with real-life examples of hacking such as getting a focused, spear-phishing email asking them to login to see their new assignment. Next, they should be given clear instructions in regard to what to if they do fall for the exploit: immediately let the school know. Being able to report and incident

may be more critical than preventing them since mistakes happen. This procedure should count as early grade, mandated for graduation. Through practice, students will understand how hackers think and get used to this as a routine measure they take daily. Hopefully, the students will take up the aware mindset needed to ensure that they keep a secure personal cyber activity.

The one aspect of cybersecurity that is well-accepted in the world is that it remains for a prolonged time. Technology is only growing, especially since with the COVID-19, the need for technological access and automation will only grow, meaning the cybersecurity issue will only grow with the rise of new hackers and more individuals seeing the potential misuses. This research is only the beginning. More research is required to assess the future students' interests, especially since how every generation has its own preferences. Next, the conclusions made regarding the solutions lack validity in regard to their effectiveness. Until tested and studied further, the best guess anyone has regarding their effectiveness is exactly that: a hypothesis. With any hypothesis, it must be tested to be affirmed. Through a cycle of testing reform, an effective system should present itself. For the time being, the suggested solutions are the most supported option available to start the process.

Acknowledgments

I would like to thank Dr. Soo Park for helping me with this project.

References

Berson, M. J., & Berson, llene R. (2014). Bringing the Cybersecurity Challenge to the Social Studies Classroom. Social Education, 78(2), 96–100. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=95720222&site=ehost-live

Center for Strategic and International Studies (CSIS). (2019). Retrieved 4 September 2019, from https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

CISA. "Security Tip (ST04-001)." Cybersecurity and Infrastructure Security Agency CISA, www.us-cert.gov/ncas/tips/ST04-001.

Code.org. (2019). 2018 State of Computer Science Education. [online] Available at: https://code.org/files/2018_state_of_cs.pdf [Accessed 28 Oct. 2019].

Smith, A. (2017). Americans and Cybersecurity. Retrieved 26 August 2019, from https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

Son, Joon & Irrechukwu, Chinedum & Fitzgibbons, Patrick. (2012). Virtual Lab for Online Cyber Security Education. communications of the IIMA. 12

Uscyberpatriot.org. (2019). AFA CyberPatriot Website. [online] Available at: https://www.uscyberpatriot.org/ [Accessed 28 Oct. 2019].

WEISER, M. and CONN, C. (2019). Integrating Cybersecurity Into The Business Curriculum | BizEd Magazine. [online] Bized.aacsb.edu. Available at: https://bized.aacsb.edu/articles/2017/01/into-the-breach-integrating-cybersecurity-into-the-business-curriculum [Accessed 28 Oct. 2019].

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Computers in Human Behavior, 84, 375–382. https://doi.org/10.1016/j.chb.2018.02.019

Yılmaz, Ramazan & Karaoğlan Yılmaz, Fatma Gizem & Öztürk, H.Tuğba & Karademir, Tugra. (2017). Examining Secondary School Students' Safe Computer and Internet Usage Awareness: An Example from Bartın Province (Lise Öğrencilerinin Güvenli Bilgisayar ve İnternet Kullanım Farkındalıklarının İncelenmesi: Bartın İli Örneği). 7. 10.14527/pegegog.2017.004.

Yin Pan, Mishra, S., & Schwartz, D. I. (2017). Gamifying Cybersecurity Course Content for Entry Level Students. Proceedings of the ASEE Annual Conference & Exposition, 6019–6028. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=125730107&site=ehost-live

Harackiewicz JM, Smith JL, Priniski SJ. Interest Matters: The Importance of Promoting Interest in Education. Policy Insights Behav Brain Sci. 2016;3(2):220-227. doi:10.1177/2372732216655542