A Survey on the Cybersecurity of K-12 Schools

Ethan D. Hills
University of North Georgia
Department of Computer Science

1 Introduction

Whenever a student sits behind an electronic device connected to the internet, he or she is vulnerable to outside threats. Computers play a crucial role in the transmission and access of information. K-12 students need protection from harmful content found on the web and a healthy learning environment. Parents must be reassured that their student's personal information is protected by the walls of the school building and that their student is protected from cyberbullying. Teachers must also educate students and parents on how they can strengthen the security of the school. This report will address how K-12 schools should execute a well-planned computer security policy while maintaining a stable learning environment for the students. Computer Security in K-12 schools can be summarized with seven solutions: content filtering, issuing strong policies, educating the students, identifying the security threat, implementing a well-planned Bring Your Own Device guideline, updating school infrastructure, and addressing social media concerns.

1.1 Content Filtering

When it comes to securing K-12 school networks, a standard approach is filtering. Content Filtering strengthens the safety of students from pornography, pedophiles, hate groups, and other threatening factors. In some cases, over filtering occurs when a school blocks too many resources, capturing some resources that do not even pose a threat to the student. K-12 schools need to take an approach that has both the student's safety in mind as well as their ability to learn new things. Before a network administrator can begin working on a secure network, there must be an understanding of what threats face K-12 students. The Children's Internet Protection Act is a federal law created in 1999 that underlines the common threats to minors. The purpose of CIPA is “to protect America’s children from exposure to the obscene material, child pornography, or other material deemed inappropriate from minors while accessing the internet from school” (Report of the Committee, 1999). When a student sits down behind the keyboard of a computer, schools must reassure parents that what the kid looks up and discovers on the internet is safe and beneficial to their learning.

The Children Internet Protection Act is a federal law that requires schools that receive federal funding to protect students from malicious content on the web. CIPA accounts for all types of explicit material that may be viewed online, and it gives examples of methods to prevent the "aggressive tactics of commercial pornographers on the Internet [that] expose children to random and unintended exposure to sexually explicit material" (Report of the Committee, 1999). In a report issued by the Senate Committee on Commerce, Science, and Transportation, “exposure of children to pornography distorts natural development by shaping sexually perspective through premature exposure to sexual information and imagery." Students are also prey to incidents involving contact with pedophiles who "utilize the Internet to lure and seduce children into illegal and abusive sexual activity (Report of the Committee, 1999)." Schools need to ensure that students are protected from pornographic media, online hate groups, pedophiles, sensitive information (like designing a bomb), and ways to grow or obtain illegal drugs. To battle claims that restricting access to information to minors is unconstitutional and is against the first amendment, the US Supreme Court has ruled many times that "schools are non-public forums that are outside the general marketplace of expression" protected by the first amendment (Report of the Committee, 1999).

Content filtering is the act of blocking access or visibility of harmful content that is classified in numerous categories ranging from gambling to pornography. When schools implement this policy, "a properly configured filter will block all content that education policy has defined as inappropriate while allowing access to sites deemed acceptable” (Malgosa, 2013). Filtering is critical to making sure that students do not find themselves exposed to the harmful content. In some scenarios, students may search for something that seems harmless, but the search returns disastrous results. The downside to filtering is the capability of "time or information lost by users due to over-filtering." Content filtering is successful when schools implement a strategy by “creating a technology bubble around kids” (Malgosa, 2013). An approach, though deemed the safest way to protect students, is to "shut everything off and not offer the services." Closing access to the Internet, of course, maybe the best solution to secure a school network but is not optimal for a student's learning experience. In a technology-driven world, access to computers is

crucial to teaching students with the technology they are familiar with comprehending. Teaching students without technology in a world that is already technology driven can be compared to teaching a student math with an abacus—a pegged calculator—rather than the scientific or four-function calculator.

1.2 Policies

Schools must design an Acceptable Use Policy (AUP) and a well-devised security plan. This policy defines what sites are acceptable and not acceptable to authorized users. The mission and goal of the AUP are to "shield students from harmful material and enable access to beneficial internet resources" (Pierce, 2012). Even the faculty of K-12 schools must have content filters to ensure that what they view cannot be a platform that indirectly affects students. The AUP defines who are the authorized users of the network as current faculty, staff, and students of the school (*IT Appropriate Usage, 2016).* The policy resources section lists all the resources on the network such as projectors, email systems, computers, and even telephones that authorized users to interact with daily. These policies underline what rules the authorized users must abide by before being given authorized access to the resources. Individual responsibilities are emphasized in the policy and feature vulnerabilities to using the resources. These can range from using resources to harass others or attempting to download harmful software to tamper with the network.

Schools must also address the problem with unauthorized people entering school buildings and trying to gain unauthorized access to the school's network from within. There must be security measures in effect to prevent an unauthorized person from getting access to the school's network. In most cases, schools give out credentials to students, faculty, and administrators to gain access to the system resources. A school should put into effect a Password Management Policy (*UNG Password Management*, 2014). This policy acts as a part of the Acceptable Use Policy, which gives authorized users the ability to access the network resources. Schools must ensure that student credentials are secured away from anyone outside of the school. Student passwords must have a required length, expiration date, and policy on storing passwords. Faculty passwords will need to expire sooner than students and have stronger

credentials to ensure higher security on teacher accounts due to the higher authorization with faculty. Ensuring that students have protection over their credentials is an important rule to teach to students within the classroom. Teachers must also be on alert that the students do not know their credentials.

With these policies in effect, teachers need to implement policies to educate their students on how to be safe on the internet. K-12 school security programs need to include "policies to protect students from the consequences of inappropriate online behaviors and teach appropriate internet behavior" (Bruder, 2014). Faculty will fail to teach students the importance of moral behavior online because they feel that "cyber-safety instruction [is] unnecessary because the school has locked down its computer systems" (Bruder, 2014). Not teaching students online behavior will fail "to [learn] proper Internet practices and will, therefore, put the schools at risk as soon as they log off the school network and log on to their personal computer or smartphone that has no filter nor adult supervision" (Bruder, 2014). Students need to know that when they go home, they still need to practice safe online behavior and steer away from anything that may be harmful to their well-being. For students to have these skills, teachers must have taught them how to be safe online through training and computer security awareness programs. When approaching computer security measures at schools, administrators need to know that "cybersecurity cannot end when a student goes home on the bus; it follows them wherever they are" (Wong, 2011).

1.3 Educating the Students

School security does not stop at content filtering. Once students are taught, filters are implemented, and teachers are informed, the school is still vulnerable to inside and outside attacks. Before implementing the best security protocols in schools, there needs to be an understanding of what information is valuable to hackers. When creating a risk assessment at a school "the primary goal is for schools to protect their ability to fulfill their educational missions" (Dark, 2004). Part of a security audit focuses on the identification of assets that need to be protected in the digital environment. Some assets in schools that require confidentiality are "student grades, health records, bank account numbers, payroll

information, lesson plans, attendance records, and online systems that provide homework updates for parents." The threat-source can be identified as "unauthorized users such as outside hackers, disgruntled or mischievous students." Schools must prevent scenarios where "unauthorized users gain access to confidential data, and can steal or modify [the data]."

1.4 Identifying the Security Threats

It is estimated that "15 percent of all data breaches happen at educational institutions" (Keep Schools Secure, 2016). Data breaches are defined as when there has been a loss of confidential information or when this information has been put at risk. Schools must protect themselves from "malware and viruses, distributed denial of services attacks, criminal and recreational hacking." Unauthorized users gaining access to the student information system attacked a school in California in May 2015. This attack resulted in the changing of grades as well as the loss of Social Security Numbers (SSNs), birth dates, and medical information. An attack in July 2014 targeted a Missouri school that compromised confidential personal information of over 10,000 students and employees such as SSNs, student records, and employee evaluations. When data breaches occur at school institutions, there are thousands of dollars involved to repair and strengthen the security. These costs "include working with experts to remove the viruses as well as the cost of notifying students and parents about the breach."

Social Security Numbers and personal information present a challenge to the security of a school. K-12 schools are considered "the most attractive targets for data privacy crimes, " and almost 150,000 students are victims of identity theft every year (Keep Schools Secure, 2016). Schools have already begun to use encryption to protect this data, but only half have done so. Having access to numerous SSNs that are fresh and with no history will inspire hackers to be involved with “websites on the Dark Net [that] will sell SSN to the discerning buyer” (Finkel, 2016). While criminals are selling student’s SSNs for hundreds, other criminals are using those numbers for even more malicious means.

While securing the computer, the network service is the top priority, making sure that the internet is fast for every student is just as important. The Federal Communications Commission (FCC) "has set a

K-12 Internet access target of 100Kbps per student" (Raths, 2016). The reason for this demand was the fact that some students had faster internet at home that was more efficient and more resourceful than at school. In most cases, the student's home internet had no content filtering or security measures like those that the school was implementing. Having a reliable bandwidth per student is the best way to approaching a fast-paced access to information on a school network. At the same time, these high-speed networks need to ensure that the information requested is both safe and quickly accessible. The primary challenge with school systems is "to harness [active] technology while staying ahead of the ever-evolving threat of a data breach of cyber-attack."

1.5 Implementing Bring Your Own Device

Another threat to school systems is not necessarily malware, but how many access points hackers can get into the mainframe of a school's internet. Schools need to address the policy on Bring Your Own Device (BYOD). Schools that allow their "students to use technology that they are familiar with encourages participation in the classroom" (Bruder, 2014). Some schools have enacted a banning on all forms of technology from home, giving a negative look of technology towards the students. Rather than implementing this policy, it is recommended to use an "If I see it, you lose it" policy. In many ways, letting a student bring their technology to school promotes many opportunities for learning that cannot be implemented in any other way. Having a policy that allows students bring their own devices to school ensures that students can advance their education significant ways. Students can "use their own devices for research, participate in audience response systems, interactive assignments, use games to understand science, store homework on the cloud, play background music through headphones to concentrate on work, and even Skype other students from foreign countries" (Bruder, 2014).

No matter if the school implements BYOD policy or not, schools must address how students' personal devices will be carried out in school education. There needs to be a written school policy that lists out in clear terms that students, teachers, and parents can understand. Having prescribed times to have the portable devices used in and out of classrooms is crucial to limiting distractions with these

devices. A common topic of debate that needs to be addressed is whether schools need to implement a ban on recording capabilities with devices as a recording of in-class activities may be threatening to the teacher or student. Confiscation of devices is necessary when the use of unauthorized devices occurs and that these devices "may be searched by parents or law enforcement" (Bruder, 2014). Allowing the students to bring their own devices from home is an excellent way to implement new ways to learn content, but is recommended to be done in a healthy way that brings support to the teacher's teaching objectives.

The more students who have access to the school's Wi-Fi network, the more toll it can put on the school's network as each device is competing for connectivity. When it comes to internet availability "students want the freedom to use their mobile devices on campus, " and they want it fast (Wong, 2011). However, the problem with adding all these devices is that "the greater the number of devices and operating systems [that are in the schools], the more vectors for infection there are." If schools do not enact the ability to let students bring their own devices to school, they will prevent infections to the school's network, but this impedes the learning experience for the students. K-12 schools should find a healthy balance. Prioritizing network traffic is crucial and can be done with improving hardware infrastructure. While students have ready access to the internet, this should not slow down the access of information for teachers.

1.6 Updating School Infrastructure

Schools need to make sure that their current infrastructure is up to date. Schools are recommended to guarantee that the programs that are readily accessible to students are secure and up-to-date. Schools need to make sure that their browser software is up to date. Finkel states that the standard vulnerable access point for hackers involves the use of unsupported software like "Explorer 5, which has not passed muster for ten years", and is prone to security vulnerabilities (Finkel, 2016). Most schools do not have strong Wi-Fi routers, and some school routers cannot manage multiple connected devices at once. Schools need to take an active approach to firewall management as well. School districts have taken

a layered approach to firewalls providing the ability to have onsite and offsite filtering, combating threats from both outside the school and inside the school. Next Generation Firewalls are a one-stop shop for most security solutions and represent the birth of a generation of firewalls. They provide ample ways to "catching threats and combining multiple functions into a single device" (Keep Schools Secure, 2016). These firewalls can target traffic irregularities through deep packet inspection to examine the flow of data. Active firewalls distinguish what traffic is beneficial for the student and allows resources for educators. Firewalls can also be implemented as content filters through their ability to block sites for recreational use and prioritize traffic by managing bandwidth. Managing bandwidth gives network administrators a central management interface to control multiple devices and applications onto one system.

1.7 Addressing Social Media Concerns

Social media is an increasing threat and concern to school networks. A detail of debate has taken place over the use and implementation of social media in the school environment. Most school districts have been utilizing resources from social media "to get situational awareness of what's happening that could affect [schools]" (Finkel, 2016). Some schools allow Facebook to be available after hours so that faculty can monitor the activity of their students. This monitoring of social media helps identify issues where students may express the need to "shoot up the school" or even cyberbullying between two students" (Finkel, 2016). Resource officers and counselors, to diffuse the problem, would approach the students the next school day. Social media also allows teachers the ability to address cyberbullying and understand the consequences of bullying on social media. Giving students the ability to understand how their words can have an influence on others online can "address everything from bullying to what it means to be a real person."

Communication between teachers and students on social media has received similar debates with its role in the educational setting. In many cases laws, "ban on teachers communicating via any non-work-related internet site that allows exclusive access with a current or former student" (Pierce, 2012). There is a saying that "if one life is saved then it is worth it" and this is how approaching social media

communication should be viewed (Pierce, 2012). Many teachers have stated that they were able to "get a message through Facebook on a Friday night from a suicidal student and was able to reach out to the internet for help." In these cases, students need to be able to communicate with teachers whom they know are trusting to get help with problems that may be happening outside of the classroom. Schools need to address whether they will allow communication between students and teachers through social media or not.

2 Hypothesis

From shielding students from malicious content to ensuring students can reach out for help using standard platforms, securing a K-12 school's computer network is a complex problem faced with moral dilemmas. K-12 schools need to guarantee parents of their students that their children are safe from predators and are not prey to unsafe content outside of the school's walls. K-12 Schools that are not equipped or trained to combat cybersecurity threats will fail to provide protection from malicious content and harm the student's learning environment.

3 Method

The method of this survey is to provide a questionnaire to IT professionals and K-12 faculty who are willing to address if there is a concern over the cybersecurity of their students. The survey will contain questions that address the seven cybersecurity concerns stated in this proposal to see if adequate preparations have been made to combat cyber threats towards K-12 students. The questionnaire will follow a five-point Likert Scale to gather responses. Surveys given to IT Professionals will address the strength of the schools' network. The results will identify whether schools have taken the time to discuss online behavior with their students and if IT Professionals have taken appropriate measures to protect their students. This research was approved by UNG's Institutional Review Board.

3 Results

A survey was conducted in 20 random counties across Georgia through the use of email. The email that was sent out is seen in Appendix 1. For the protection of each county, I will not release the results of each individual county, but I will report a broad picture of what is being seen in counties as a whole. I emailed each IT Director to get feedback on their views of cybersecurity and how their IT System reflects those views. The survey hit some backlash as the email was often perceived as a phishing attack. The survey took only 2-5 minutes to complete and covered different aspects of IT cybersecurity as discussed in my literature review. A sample of the questionnaire is seen in Appendix 2.

Physical security results showed that there seems to be a strong sense of physical security of IT Systems as equipment is disposed of with security/discretion, IT Systems are locked behind secured doors, and alarm systems are engaged. There was some uncertainty on whether IT teams would be notified when an unauthorized user gains access to onsite workstations this is probably due to the format that county IT teams are centrally structured rather than present at each school location. There was also some uncertainty on whether IT equipment is permanently marked with an ID number.

Updating Systems had positive feedback as all counties reported that their systems are adequately updated getting rid of a common IT weakness. There was some uncertainty on whether policies stated whether IT teams should monitor software updates. All schools have a strong antivirus running and most schools reported that their infrastructure is up to date.

The policies section was supposed to bring back all positives but was met with some uncertainty. Some counties reported that their Acceptable Use Policy was not clearly defined or readily available to faculty. This question was supposed to be on the agree side but was met with mixed opinions. Some counties reported that they did not have a disaster recovery plan in place and that if there was a disaster where their systems were disrupted, that they would not have a plan to regain connectivity. Most schools implemented a well-defined Bring Your Own Device and most school districts included this written policy on their county school website. Most counties reported that their acceptable use policy is readily available to the students. It seemed that the schools that reported that did not have a policy for the

students saw no reason to have one. This may be presented with a problem as students need to understand what is defined as acceptable use when gaining access to the network. Most schools reported that there was no policy for temporary access to IT Resources. Hopefully, this was answered as not giving temporary access to visitors as this is not needed. In my research I found cases were schools gave access to vendors and visitors.

Security awareness should have been present at all the schools, but it seems that this aspect does not receive as much attention as it should. Most counties reported that the schools may have a security awareness and training program for faculty, but not strong enough to make an impact. Most counties reported that teachers included teaching online behavior in the student's curriculum, but it is not strong enough to have a definite agreement. Students are educated to understand that cyberbullying is bad and that they know who to reach out if they are a victim. Security awareness seems to be the common weakest link in most counties.

Password Management had a lot of positives as there are strong password management policies being implemented. Password policies are clearly defined, though they are not readily available to faculty and students. Some counties felt that their password policy was not strong enough and needed to be improved to keep information safe. Most counties reported that their workstations include an automatic screen lockout after there has been no use.

As predicted, content filtering was the most positive of all the categories included in the report. All counties reported that they have a content filter in place to comply with CIPA. However, there were mixed views on whether their content filters improve their student's education or hinder it. Schools will need to reassess whether their content filters are proving to be efficient or overbearing towards the student's education.

4 Conclusion

The purpose of this survey is to determine if schools have protected students from cybersecurity threats and whether schools are adequately equipped to address these means. K-12 Schools that are not equipped or trained to combat cybersecurity threats will fail to provide protection from malicious content and harm the student's learning environment. The questionnaire was divided into six sections: physical security, updating systems, policies, security awareness, password management, and content filtering.

Results showed that public schools are meeting the baseline requirements of a secure IT infrastructure. To improve cybersecurity in K-12 schools, I propose adopting a program that follows the SECURED acronym. As my thesis discusses the seven points of K-12 school cybersecurity, the SECURED acronym will aid in making sure that a school's infrastructure is secured past the baseline. The seven letters address issues on Social media, Enforce policies, Content filtering, Update systems/infrastructure, Realize threats, Educate users, and Device policies. These seven points are mentioned in my literature review and provide support to improve the current public schools' view on cybersecurity.

5 Acknowledgements

I would like to personally thank my honors thesis committee who aided me in my research: Dr. Bryson Payne, Dr. Ahmad Ghafarian, and Dr. Gina Childers. Also special thanks to all the directors of each school district who assisted me in my research.

6 Closing Notes

This project was approached with difficulties that would have to be reassessed if a similar project was conducted. One of the problems did not have the response rate of the survey as hoped as most directors believed that the survey was not credible. Some counties did not even list their email addresses of the IT Directors. This may be a problem as teachers or outside faculty may need to get in touch with an IT official but will not have the ability to do so. Overall, I was satisfied with the outcome and I learned a lot about the cybersecurity of K-12 schools.

X Appendix

X.1 Email

I am Ethan Hills, a computer science student at the University of North Georgia. I am conducting a questionnaire for my Honors Thesis on the cybersecurity of K12 schools. The survey touches different aspects of cybersecurity topics and only takes 2-5 minutes to complete. It is entirely opinion based and features no personal identifiers except county for analysis. Completion of the survey will assist in understanding if schools are taking appropriate measures to secure IT Systems. I would greatly appreciate if you could take a look at the questions before sending them to your IT team.

If you have any questions about the survey or my honors thesis please do not hesitate to ask. You can email me or my honors thesis chair Dr. Bryson Payne if you have further questions. This study is approved by UNG's Institutional Review Board and is not sponsored by the Board of Education.

I appreciate you taking the time to assist me with my honors thesis.

Thank You,

Ethan D. Hills
University of North Georgia, Senior
Computer Science Major

X.2 Survey

Physical Security:

When disposing outdated equipment, it is done so with security and discretion.

We become aware when an unauthorized user gains access to onsite workstations.

The physical location of the computer and other IT rooms are setup to ensure security.

Our systems are protected by secure physical security such as locked doors, alarms, etc.

All school equipment is permanently marked with an identification number.

Updating Systems:

Our systems are adequately updated.

Our policies adequately state that we should monitor software updates.

We have a strong antivirus system running.

The current network infrastructure is up to date.

Policies:

Our acceptable use policy is clearly defined and readily available.

In the event of a disaster, we are able to locate our disaster recovery plan.

Our policy on students using their devices on the network is strong.

Our acceptable use policy is readily available to the students.

The school has policies for temporary access by employees, visitors, or outside vendors.

Security Awareness:

The school sets forth a strong security awareness and training program for all faculty.

The school includes computer security and behavior in the students' curriculum.

Computer Security programs are provided for students.

Cyberbullying programs are provided for students.

Password Policy:

Our password policy is clearly defined.

Our password policy is readily available to faculty and students.

Our passwords have a defined expiration date.

Our password policy keeps our information secured.

Our systems use an automatic screen lock out.

Content Filtering:

The school utilizes monitoring software linked to workstations to view activity

We have a content filter in place to comply with CIPA

Our content filters improve a student's education.

Computers include filters to monitor internet activity on school computers.

Bibliography

Bruder, Patricia. *Gadgets Go to School: The Benefits and Risks of BYOD (Bring Your Own Device)*. Michigan: Education Digest, 2014.

Children's Online Privacy Protection Act. Washington DC, 2002.

Dark, Mellissa. *How to Perform a Security Audit.* Ohio: Technology and Learning, 2004.

Finkel, Ed. *In School Security, Cybersecurity and Social Media a Growing Concern.* Michigan: Security: Solutions for Enterprise Leaders, 2016.

IT Appropriate Usage. Georgia: University of North Georgia, 2016.

Keep Schools Secure to Keep Learning. California: The Journal, 2016.

Melgosa, Annette. *School Internet Safety More than 'Block it to Stop it'.* Washington: The Journal of Adventist Education, 2013.

Pierce, Margo. *Equal Measure: Shielding Students and Enabling Access.* California: The Journal, 2012.

Raths, David. *Better Connections*. Arkansas: Public CIO, 2016.

Report of the Committee on Commerce, Science, and Transportation on S. 97. Washington DC: US Government Printing Office, 1999.

UNG Password Management Policy. Georgia: University of North Georgia, 2014.

Wong, Wylie. *Balancing Act: Access v. Security.* California: Baseline, 2011.