Spring 2017

Cyber Security Risks in Public High Schools

Ion Goran
CUNY John Jay College, ion_goran@yahoo.com

Cyber Security Risks in Public High Schools

An Applied Research Project

Presented in Partial Fulfillment of the Requirements

for the Master of Science in

Digital Forensics and Cybersecurity

John Jay College of Criminal Justice

City University of New York

Ion Goran

February 2016

Cyber Security Risks in Public High Schools

Ion Goran

This Applied Research Project has been presented to and accepted by faculty of the Digital Forensics and Cybersecurity Program, John Jay College of Criminal Justice of the City University of New York in partial fulfillment of the requirements for the Master of Science in Digital Forensics and Cybersecurity.

Richard Lovely

Thesis Advisor Signature Date

Adam Scott Wandt

Second Reader Signature Date

Douglas Salane

Program Director Signature Date

Table of Contents

Abstract

Today, just like other organizations, schools are vulnerable to cyber-attacks. This vulnerability has vividly revealed itself in recent years, with the number of attacks on public schools increasing and taking ever-changing forms. Today, the student's grades, disciplinary notes, learning diagnoses, phone numbers, addresses, and another identifying information is all at risk of being exposed. Moreover, poor network security poses a dire threat to parents of school children whose personal records contain sensitive or dangerous information. The practical implications of these attacks require intervention or remedy to increase cyber security. Cyber-attacks may take place when storage facilities or infected devices are introduced into systems. As well, accidental or malicious activities by operators expose or change private data about students' mental and emotional health, future postgraduate pursuits, and social security numbers. To examine the impacts of poor cyber security in the context of schools, this paper employs a case study of an urban high school and examines its vulnerabilities to various cyber-attacks and offers practical recommendations and measures to counter them.

Key words: school, cyber, security, risks, threats, network

CHAPTER 1

INTRODUCTION

Background

Companies and individuals increase their liability when their digital device is connected to other computers via local area or virtually through a network. The more devices connected to these networks, the more vulnerable the data becomes because the risk of being compromised increases directly with the increase of network traffic. In academic settings, many individuals (students, faculty, and guest) are linked to the same virtual network and/or are connected via a local area network, exposing copious amounts of sensitive data. This data can range from an individual's credit card number to a student's grade, or even a social security number.

This paper will explore some of the many ways public schools, and in particular public high schools are vulnerable to compromise of their mission and data given today's increasing use of technology in nearly every aspect of the classroom and school administration. It will suggest specific policy recommendations that local information technology personnel responsible for school networks and data systems should pursue to mitigate cyber risk. It will also suggest recommendations that local and federal agencies should pursue to mediate threat impacts. Given the ever-changing face of technology in the classroom, these scenarios serve to underscore the fact that no facet of our education system is safe from invaders. Efforts to mediate these impacts should therefore not just seek to install the necessary defensive weapons against cyber-attacks (although these measures are obviously essential), but should more holistically look at how technology is being used to educate our children, analyzing the potential issues that arise when our public educators so readily embrace new technology.

Aim of the research

"To analyze the cyber security problems in a public high school and to propose practical solutions"

Research questions

- What is the cyber threat landscape of public high schools?
- What are the particular cyber security requirements of the school and its users?
- What mitigation measures can a public high school adopt when network security is compromised?
- What steps can be taken in order to manage e-security?

Methodology

After a general review of the cyber threats that a public high school faces in Chapter 2, this paper will address the particular threats of a given school and how they can be managed and mitigated. Chapter 3 provides a case study of the information technology systems in place at an urban high school with which the author has personal and professional experience. A pseudonym for the school, Gingerwood High School (GHS), will be used to follow customary practice in reports based on participation observation. Thus, the analysis of school cyber threats, policies, and software and hardware systems in use, security practices and incidents will be primarily based on information gained from participant observation of the author in the school's everyday operation by virtue of his status as a member of the IT staff in the school. Suggestions for enhancing the cyber security of the school will be discussed in Chapter 4 based on these observations and constrained to reflect the realistic limitations of school resources. Chapter 5 will go beyond GHS and consider some general policy suggestions to enhance cyber security in public high schools.

CHAPTER 2

Cyber Risks in a High School

2.1. Cyber-attacks in the contemporary era

This chapter will provide a general overview of the cyber risks that public schools face. In August 2013, the Kentucky Department of Education's statewide Infinite Campus information network was targeted by hackers with a DOS attack, also known as a 'denial of service' attack, notoriously known for shutting down the primary source of data management and operation systems for the state. Although state officials eventually outmaneuvered the attack, the attack effectively shut down an essential component of the state's education services for an entire day, limiting the services schools could provide (Lestch 2015). Taken with attacks throughout the country that halted the administration of standardized tests, this displays how security breaches are not the only fear schools should have – they must also be prepared for the threat of destructive forms of hacking as well. While the scope of this attack attracted media attention the risks to individual schools are also great, albeit less noticed.

2.2. Vulnerability of schools to cyber-attacks

Perhaps no governmental body is more vulnerable than public schools because public schools have rushed into adopting computer technology for instruction and management without sober concern or resources to manage the security risks. This vulnerability of individual schools has vividly revealed itself in recent years, with the number of attacks on public schools increasing and taking ever-changing forms. Many districts, for example, have had their students' or teachers' information entirely stolen or compromised. In 2013, this type of attack occurred when 15,000 students at Sachem School District in New York had their personal data posted to an online forum. In June 2014 when hackers obtained student information from a charter school in Jersey City, New Jersey, including social security numbers and from students at public schools, and in November 2014, when Prince George's County public schools in Maryland had 10,000 of its employees' information compromised (Lestch 2015). Administrators, many of them veteran educators with little technological experience, have been at a loss as to how they should address these problems, placing thousands of teachers and students at future risk.

Moreover, still more hackers have intentionally taken advantage of the new uses of technology in the classroom and administration to disrupt normal functioning. In particular, with federal Common Core State Standards instituting computerized standardized testing in states throughout the country, hackers have seen prime opportunities to wreak havoc on students and administrators. In states throughout America, including Florida and Alabama, state administrators have had their exam dispersal thwarted because hackers infiltrated their network and shut down the server needed to provide the tests (Dumas 2015).

A. *Concerns regarding the security of students Security of Students*

Cyber-attacks have also raised the concerns regarding the security of students. When parents send their children to school they are transferring to the administrators and teachers their parental responsibility to protect their children. It is, therefore, the school's necessary duty to take all required measures to ensure students' safety, which explains efforts to install metal detectors and security devices to detect and prevent dangerous behavior among students or threats from outsiders. The institution must ensure the privacy of each student is secure by limiting the possibilities of a breach. Without effective security, students, teachers, parents, and those involved increase their liability as well as risks from malicious cybercrimes that can affect their professional or personal life.

Throughout the country, over the past five years, there has been a marked increase in the use of technology in schools with the goal of enhanced student's physical security. From 2013-14, 75% of schools across the United States used one or more surveillance cameras to monitor the school, up from 61% in 2009-2010 (Fast Facts). The portion of schools that have an automatic electronic system to alert parents of a school-wide emergency has also increased, from 635 in 2009-10 to 82% in 2013-14. Today, 93% of public schools have access to school building controlled, often electronically (Fast Facts). The ironic result is school security now depends upon the effectiveness of technology that introduces cyber risks to the school. .

B. Risks regarding information accessed or compromised

Teachers and students are also at risk of getting their information accessed or compromised through a security breach. The potential for sensitive information getting breached and stolen from educational institutions is very real in the United States. According to the Privacy Rights Clearinghouse, from 2005 to August 31, 2013, there were 695 breaches at schools throughout the country that potentially disclosed over 11 million personal records (Alao 2013). With unauthorized access to school computers, , hackers can access personal files that are on the desktop or the network it connects to, whether from out of curiosity or malice.

C. *Frauds during financial transactions*

Not only are school databases about students and faculty vulnerable but schools that maintain finances on a network are vulnerable to financial frauds during financial transactions. According to the Census Department, a total of $530.6 billion was obtained in revenue in 2013 by public elementary through secondary schools (U.S. Census Bureau). That means that together, all of the schools in the United States are more valuable than the world's eight most valuable brands combined. Indeed, the cash flow is more than three times the size of Apple ("The World's Most Valuable Brands"). Included in this overwhelming flow of money are numerous sources of liquid cash. For example, in 2013, according again to Census data, public schools maintained $182.1 billion in cash and securities (U.S. Census Bureau). Taking into consideration the $182.1 billion dollars of capital and securities is a substantial amount of money that is constantly being managed and handled by schools, often on a computerized network. Furthermore, included in the $520.6 billion are pension costs, sent in checks to retirees and administered most of the time by the school districts themselves. In 2015, public schools are projected to spend nearly $52 billion on pensions for these retirees (Costrell 2015).

This is no longer just a risk as a major theft of public school funds has already occurred in the United States, albeit with less fanfare than the other main cyber thefts as of late. In December 2010, hackers electronically stole $2.8 million from the Duanesburg Central School District in upstate New York (Alao 2013).   While the larger budgets of school systems are more attractive as targets, local schools that maintain their finances online are also vulnerable to cyber theft.

D. Risks for Standardized Administration of Test

Test administration is also vulnerable to hackers' attacks. In the United States, over 40 states across the country have adopted Common Core State Standards, which detail what math and reading skills students should be able to know at each grade level. As part of this new system, there are also a series of new, computerized tests, referred to as the Smarter Balanced Assessment Consortium and Partnership for Assessment of Readiness for College and Careers. These computerized tests, while controversial, have defined benefits, such as the fact that it allows the set of questions to change depending on a student's answers to others. These computerized tests enable students' test experience to be personalized so educators can obtain a clear picture of individual student abilities and aptitude (Meehan 2014).

However, this use of computers has spelled trouble for numerous schools throughout the country as hackers have messed with test administration, in some cases shutting down the entire testing process. For example, in Swedesboro-Woolwich School District in New Jersey, hackers prevented elementary school students from taking online statewide tests in a so-called ransomware attack (McDonald 2014). Similarly, the Mobile County school system in Alabama experienced two 'denial of service' attacks in April 2015 that interrupted their standardized testing. The threat is not only to Common Core testing as in March 2015; Florida state officials announced that similar attacks had halted the administration of Florida Standardized Assessments to students (Rodriguez 2015).

2.3. Students as potential hackers

Many cyber security threats facing schools are from the very students they serve. Students are young, curious individuals who are eager to learn and identify themselves during their years of growth. In recent statistics, there is a substantial amount of students venturing into programming, to about 18.5 million individuals, with 11 million professional software engineers and 7.5 million hobbyists (Ranger, 2013). While hacking in and of itself can be a productive activity for young people, some student hackers turn their attention to cracking school systems and have committed petty crimes, such as of changing their grades on public schools' online system. Although university students committing such crimes are nothing new, younger high school students have also been able to override school firewalls and tamper with their grades. In 2015 alone, students at Dixon High School and San Dimas High School in California, New Dorp High School in Staten Island, and Churchill High School in Maryland have all been caught hacking computers to change their grades (Chang 2015). These attacks, while an obvious threat for a school district, underscore the glaring vulnerabilities in school security networks. Threats exist from not only young students who attend a given school but from more advanced foreign hackers, only with more malicious intent.

2.4. Why are cyber invaders difficult to stop in school premises?

Schools are so detached, decentralized, and underfunded it makes it more difficult for them to address the specific security needs they have. As Michael Alao notes "Public school districts alone are not responsible [for addressing cyber security risks]…because the risks that make public school districts especially vulnerable to cybercrime may require state or state agency action to address. Financially strapped school districts already face the challenge of maintaining an adequate teaching staff without adding the financial burden of addressing cyber security (Alao, 2013).

Our public schools are too preoccupied with meeting the basic educational standards given to them to pay adequate focus on the seeming abstract and remote cyber risks inadvertently introduced from the technologies they adopt to meet those standards. To review those cyber risks in the next chapter we turn to the case study of a public high school.

CHAPTER 3:

CASE STUDY- GINGERWOOD HIGH SCHOOL

3.1. Overview of the school

Not only must schools suffer through the lack of technological resources and preparedness that all local governments must deal with, but they also are particularly vulnerable due to the many unique ways technology is integrated into their predictable, easily accessible programmatic structure. Furthermore, they are unique in that they involve millions of our most vulnerable citizens: youths. Young students today are ever more connected to social media and cell phones on a regular basis, but they are not more conscious of the risks or worried about potential security breaches (Murray 2014). Furthermore, as young people continue to use cell phones fewer schools are banning their use: in 2013-14, 76% of schools prohibited the use of cell phone and text messaging, down from 91% in 2009-10 (“Fast Facts” 2014). Therefore, in many ways, public schools are uniquely threatened in a way that other public and private entities are not, and until now many of these risks lack detailed research.

To illustrate the cyber risks and challenges that face a public high school, we will consider the situation in an actual high school, which we will call Gingerwood High School (GHS), a suburban high school of 1,600 students, in an upper-class suburb of a major U.S. city. Gingerwood is a multifaceted and diverse community.

3.2. Current Situation of Security Infrastructure and Faculties at Gingerwood

Although regarded as a desirable community, urban problems, such as drug use, are on the rise. There is a trend of painkillers and heroin being introduced to the younger Gingerwoodians. As well, debilitating addictions among parents tear apart some families. A trend is to introduce more technology to resolve problems that arise for the school which brings increased cyber risk to the school.

Last year, a student at GHS was found to be high on painkillers and in possession of a steak knife, allegedly due to a drug-induced accident. Due to community uproar after this incident, the school reacted by looking toward technological solutions. It installed metal detectors at the student entrance to the school and security cameras in every hallway and most classrooms. The installed system provides digitized archives from security cameras and other devices in service. These cameras were bought from outside and are maintained by IT staff. The cameras in the classroom raised concerns by faculty that they might be misused by administrators but they were effectively handled after addressing their concerns. However, owing to the absence of any proper security procedures such as effective security of camera and data rooms, the system is vulnerable to direct breach by internal or external hackers.

3.3. An Overview of IT at Gingerwood High School

GHS has a total of 1,600 students and 30 faculty staff members. Both students and teachers use the internet whenever they get free time. The school database is managed by the IT staff. Teachers usually make queries of the database whenever they want to know the details of students or when they want to check their profiles. The IT staff is comprised of two individuals who also have teaching responsibilities. The role of the IT staff is primarily to serve the educational mission of the school; however, whenever a new security or IT system is employed in the school, teachers and students are provided an overview by IT staff through Power Point presentations.

There are in total 2 servers, 100 desktop PCs and 30 tablets owned by school. The desktop PCs are present in the labs accessible to both teachers and students. The server rooms are secured well but lack effective measures against internet hackers. Students usually use Microsoft World and Power Point for academic purposes. Teachers and staff also use this software.

Gingerwood, like many schools throughout the country, has integrated technology into nearly every aspect of daily life, not just security. Indeed, its entire scheduling system runs on technology to include the bell system that maintains the class schedule, the announcement system that connects the administration to students in every room, and the televisions in classrooms and hallways that provide updates and information to students. The fire alarm system is also hooked up to a centralized database so it can be accessed and disabled if necessary by the administration.

To access the internet, Internet Explorer is used. The school has hired broadband services from a local ISP. Only desktop PCs are connected to internet via Ethernet while the rest of the devices such as tablets and mobile phones are connected via Wi-Fi with connection of 10 MB. At a time 50 people can be connected to Wi-Fi router. Teachers and staff are required to use VPN to access the school's database from outside. In addition, students and staff are allowed to stream movies, play games, etc. over the school network. In addition to the integrated bureaucratic system that educators and administrators in the school connect their laptops to the virtual or private network to access their classrooms, GHS teachers are also given tremendous leeway to sample new applications and technologies for their students, such as Castle Learning Online and Schoolnotes. Indeed, teachers regularly employ these new education apps and computer programs to store, analyze, and share students' answers and thought patterns, often even using students' phones to engage them on a more personal level.

Presently, the school has "Packet Filtering" firewall in place. The primary purpose of this firewall is to filter traffic that has not been specifically allowed. To access the database of students and teachers, both students and teachers provide their logins. Access to the school's networks is authorized to IT staff only. There are two IT persons who are also faculty members who teach computer science and perform their duties alternatively with 50% of their time on IT work. Both are MS in Computer Sciences and have the experience of 5 years in managing network security. They also give the information to both students and teachers whenever new IT system is employed in school.

In GHS, the entire administration's bureaucratic system is computerized into one integrated system that includes a relational database of both student and educator identifying data. The database was developed in 2011 in Structured Query Language (SQL) to query data.

The services of the local vendor and the developer, Devart, were used for the development of database management software and database connectivity solutions. The developer added indexes to database for faster querying, making relational database performs well even when the amount of data increases over time. The aim of database was to connect teachers with parents as well as to organize student grades so that they would be publicly accessible to parent.

Currently, the database system connects all relevant health service providers with guidance counselors, retired teacher pension administration, standardized test preparation, administration, and score distribution, or other miscellaneous matters relating to student attendance. Not only is this database fully integrated, but it is also readily available and user-friendly as well, with specific features installed to ensure that parents can easily access the information they need from home, for example. These types of databases are imperative for parents, teachers, students, and other vital party members who utilize this system. However, it seems fair to say that scant attention is paid to the threats these systems pose compared to their value as conveniences.

3.4. Understanding the Threat Landscape at GHS

GHS is ill-equipped to defend against a hacker. The school functions that are vulnerable to hacker attacks fall into six main risk categories: general educational disruption, students' physical security, students' personal information security, teachers' personal information security, financial management, and standardized test administration. The following sections consider those vulnerabilities. Policy changes that could ameliorate them will be considered in Chapter 4.

i) Malicious technical attacks

"Malicious technical attacks" – these may comprise outside efforts to compromise systems of GHS through techniques like attempts of physical hacking, propagation of malware (for instance Trojan horses), or Distributed Denial of Service (DDoS) attacks. These outbreaks may impact the systems and data of GHS, can employ systems of school to mount additional outbreaks on other structures, or can employ systems of GHS for unauthorized or illegal uses, causing damage to reputation. For instance, currently there are "unpatched school web sites" that could be employed to host malevolent material. Also the PCs in the school are unguarded and unpatched which means they are vulnerable to the installation of malware and can be used in "botnets".

In Gingerwood, computers can also be employed for activities such as parallel processing which enables them for use in such illegal acts as cracking of passwords in contravention of the "Computer Misuse Act". Likewise certain computerized outbreaks may impact GHS with unmanaged susceptibilities – the inadequately secured networks of school are also as vulnerable to these types of outbreaks as any other system. These dangerous attacks may obstruct functioning of GHS and need swift movement and delicate care to lessen harm. Furthermore, the fact that teachers at GHS, similar to those throughout the country, are more readily using new, untested, and often insecure methods of technology integration in the curriculum makes cyber security risks all the more severe, and their scope immeasurable.

ii) Internal attacks

Gingerwood is also vulnerable to various internal attacks. Again, the unguarded and unpatched PC's at the school are vulnerable. These attacks may take place when storage facilities or infected devices are introduced into systems and accidental or malicious activities by operators who can tamper and access private data about students' mental and emotional health, future postgraduate pursuits, and social security numbers. For instance, "keystroke" can get confidential, private inputs from keyboard like passwords and usernames.

iii) Overly simple and accessible security systems

In Gingerwood security systems are overly simple and accessible which can easily be breached by hacker. The education network is used to cater to all the individuals on campus. However, it may tend to fall victim to hackers because of the poor security structures. It is hard to create a robust system that allows for transparency and relationship formation with parents while also blocking out unwanted intruders, especially given that Gingerwood does not have the same resources that larger government and private schools do. Although transparency is key when managing this delicate situation, it is complicated to provide both transparency and anonymity, considering they conflict with each other. Although the ability to be transparent is possible, by providing the students and faculty with devices owned by the school under the condition the staff and students are unable to modify the device, he practice is currently absent in Gingerwood. However, the schools' IT department monitors the daily activity,

iv) Poor Student Security

Gingerwood currently lacks adequate student security measures. GHS does not ensure that their staff and students' privacy and sensitive data are well guarded. It even has very loose monitoring by outside and inside sources. Today, there is a need to increase the safety parameters to the virtual world, the devices the school uses such as iPads, PC's, projectors, tablets, and other vital resources in order to ensure security of students.

v) Ineffective database security

GHS servers hold information about their students that may not exist anywhere else in the world, and put into the wrong hands that information could ruin someone’s life. Because of lack of effective measures against threats such as “SQL Injection vulnerabilities” to the current database of GHS. Because of this, the student’s grades, disciplinary notes, learning diagnoses, phone numbers, addresses, and another identifying information is all at risk of being exposed. Moreover, this poses a dire threat to parents whose personal lives contain sensitive or dangerous information. The school's database developers added Java support as a measure against SQL Injection vulnerabilities; however, it is still vulnerable to anyone who can get the system to run whatever Java he chooses.

vi) Lack of Secure Personal Information Security infrastructure

While threats to individuals’ safety and the overarching, menacing possibility of a large-scale cyber-attack on Gingerwood's servers are daunting, perhaps a more realistic threat to GHS is the possibility that hackers can gain access to the massive amount of sensitive information they hold. For not only are class tests and grades available for hackers to access and tamper with, but personal information about students’ mental and emotional health, future postgraduate pursuits, and social security numbers (which are highly valuable once a student turns 18) might also be at stake. Moreover, this does not just impact students but also parents, whose personal information and emergency contacts may also risk compromise while in digital form in summary reports written by guidance counselors. Indeed, the amount of information that hackers could obtain from student files could extend well beyond what may be considered common knowledge.

In addition, lack of secure Personal Information Security infrastructure at Gingerwood may result in divulgence of all types of information about teachers. Although the kind of information that they might obtain may be different from students', they pose a more immediate threat to GHS faculty. For while the social security numbers of students would not be very usable for hackers who want to use student identities to open credit card accounts (unless they wait until the student turns eighteen), for teachers, the risk of identity theft is very real. If given access to employee information, which could contain not only social security numbers but also their bank account information. With such information, hackers could steal their identities, ruin their credit, and indeed ruin their lives.

vii) Social engineering

The last of threats to GHS, would be vulnerability to social engineering which may arise from cultivated disclosure of an interior flaw or password or "phishing" websites or emails intended to get identifications from unsuspicious users. Several experts of security consider that the major hazard to any system remains to be a careless or ignorant operator or careless users.

CHAPTER 4

ACTIONS AND MEASURES

This chapter proposes a set of measures and actions we will call an "E-Security Approach" (ESA) to address the cyber security threat landscape noted in Chapter 3. The ESA entails systematic policies and practices for sound cyber usage, incident response, and **r**isk management. While the proposed ESA is based on the author's experience at Gingerwood High School it could apply to other high schools or organizations that require keeping their network facilities, users and data safe.

4.1 Network Security

i) Data risk management regime

- School IT personnel should establish and maintain an ESA or systematic methods for usage, incident response, and **risk management**. The ESA should include development and a means to promote an "Adequate Usage Policy" (AUP) handbook for the school's information technology in a handy and easy to understand format. This Handbook must be provided to all pupils and staff.

ii) Protected configuration

- Hardware and software must be installed and maintained within guidelines for protected configuration.
- Guidelines for protected configuration must include keeping an inventory of all IT software and hardware.
- A process should be developed to ensure procedures and policies are being implemented correctly and assure that all modifications are sanctioned, recognized and applied properly. This process must include procedures for checking that timely systems updates are applied as needed; e.g., when various software versions (comprising plugins, web browsers and operating systems) are installed, when "security patches" turn out to be accessible or when software or hardware expires.
- Software, operating systems and hardware must be provided configuration protection to avoid access to services which can be employed to breach security of network, either accidentally or maliciously. For example, mobile phones provided to staff by the school should be secured to provide comprehensive password and locking guidelines.

iii) Security of Network

- Safeguard the network by using effective “firewalls” (of which an additional explanation will be provided later in this report),

- Filtering of website traffic over the network is required for avoiding websites that may introduce malicious material, checking for malware and antivirus, establishing and monitoring suitable interior configurations of security of network, e.g. via the separation of system resources.

- Security of Wireless networks requires assuring frequent changes of passwords by users and network administrators to avert accessibility from unsanctioned devices and users. Monitoring of user network access and activities is required, with notification to every user that his/her use of the network might be supervised in accordance with the AUP. This notice is indispensable and must be repeated so all students and teachers are conscious of and comprehend the AUP.

iv) Management of privileges of students and teachers

- Monitoring what students and teachers may and may not do on the system is an essential part of ESA. System privileges of students and teachers should be set so every user can acquire the services he or she needs while minimizing the prospect for accidental or deliberate network misappropriation.

- “Password Management Processes and Policies” for user devices and programs must require and confirm both that PINs are strong and robust (that is to say they are not simple to predict either physically or by means a dictionary outbreak).

- An “Automated User Provisioning System” (AUPS) should be used to manage, create and remove accounts of users when they are no longer required. Such a system should robotically erase accounts of users that have graduated or left the school, an area which is frequently ignored.

- The AUPS must be revised on a regular basis and restructured when needed.

v) Education and awareness of students and staff

- All students and staff should comprehend that their responsibilities and obligations regarding e-security and training and education are vital if security is to be attained.
- A "User Security Policy" must be developed and coordinate with the Adequate Usage Policy (AUP) related to information technology. Processes of induction and training must be accessible for every new user (students and teachers);
- Novel hazards continually surface, thus Adequate Usage Policies should be revised and restructured on a regular basis.
- Remote accessibility to network facilities of school (e.g., distant accessibility options for teachers for the management of school), must be facilitated but with adequate concern for security, to include sage of detachable personal/media devices in school and Password Policies.
- Every user must be made conscious of and comprehend any penalizing sanctions and processes for misappropriation in the occurrence of malevolent incidents regarding e-security.
- A robust e-security culture must be nurtured to minimize the usage of penalizing sanctions and processes by assuring everybody comprehends cyber risks and their particular obligations to protect the school from them.

vi) Management of Incidents

- Incident response procedures and plans must be prepared beforehand by IT staff to facilitate classifying, monitoring, reporting on, and handling incidents regarding e-security with the goal of minimizing harm and getting operations back to usual as soon as possible.

- When incidents occur, IT staff need to need to consider and document the 'lessons learned' so as to avoid related events from happening another time. IT personnel should then apply lessons learned in a wide context. For instance, it might be essential to renew a configuration of firewall after an occurrence. This might cause an appraisal of processes of patch management and configuration. Likewise, based on lessons learned it may be essential to revise the Adequate Usage Policy , which then results in an update and review of awareness and training methods for students and teachers regarding e-security. These methods may include raising awareness and training via introducing new courses on cyber security by arranging seminars and workshops for teachers.

vii) Prevention from Malware

- Effective protection from malware is required by using effective tools filtering of websites to avoid accessibility to identified malevolent webs and likewise boosting proper behaviors of users such as web browsing, opening emails and usage of detachable devices in GHS. Once again, training and education of students and staff regarding the Adequate Usage Policy of school is vital.

viii) Appropriate Monitoring

- Checking activities of students and staff, network traffic and systems, permits outbreaks and other occurrences related to e-security to be distinguished rapidly, permitting an effective and rapid reply in accordance with particular processes of management of event.

- Similarly, it is important for IT personnel to save “event logs” as possible indication in handling an undetected transgression.
- It is also significant that IT personnel review the results from checking systems and respond to alerts and alarms. Alarms, logs, and reports are inadequate if none is liable for or has the time to reply to them. Ways for accessing and storing information from monitoring should be kept in view, as systems of monitoring can quickly produce huge chunks of information.
- Monitoring procedures for activities of students and staff should be capable to notice illegal, malicious or accidental use and must be capable to recognize the users, the action that encouraged the alert and the service or data the person was trying to acquire.

ix) Detachable personal and detachable devices

- It is vital to regulate what can go into and leave the school by means of personal and detachable devices to mitigate the risk such devices pose as they are extensively employed in the school. The risks to be mitigated include dangers of theft of detachable devices, leakage of information, and the prospective of introduction of malware. This will require regulating what information can be saved on which kind of device along with policies for encrypting detachable devices and or protect distant accessibility to information.

x) Working from Mobile and Home

- Cyber security must not limit students and staff access to the school network from home or elsewhere, or from different types of equipment, in order to prolong opportunities of learning and manage functions of administration.

- An important problem in this context is dealing with “Bring Your Own Device” where students and staff desire to attach the particular devices they bring from home to wireless networks of school.

- Hazards result from the potential theft or loss of laptops of teachers and the possibility for accessibility to and escape of sensitive data from devices with restricted features of security. Educating students and staff is supreme in this context; practical approaches might comprise encrypting devices owned by school to avert illegal use and access.

4.2. Maintaining and Managing Firewalls in Gingerwood High School

As mentioned under security of network in the preceding section, the school needs a firewall to avoid illegal exterior accessibility to its systems and data. Firewalls need recurrent changes in configuration to permit accessibility to different applications and services needed by Gingerwood; IT personnel in the school may be required to confirm that any such changes in configuration do not disturb total security of network. IT personnel can deploy firewalls in the following two main manners:

- **An Integrated Positioning**, in which the firewall is positioned inside a Centre of data or other main location within network to which the broadband service of GWHS links; or

- **A Local Positioning**, in which the firewall is positioned on a system or an appliance inside premises of school, either as a part of another arrangement (like a filtering resolution) as a separate technology.

A main consideration in either circumstance is the on-going administration and configuration of the firewall. The consistency, quality, and organization of security and firewall services are the most important aspect in safeguarding that firewall endures to guard the network and its user’s data. Instead of in-house management, the school can outsource the management of firewall to a third-party. In this case following aspects should be considered during the selection of third party.

- The “**service level agreement (SLA)” should be** provided by the Gingerwood High School to a third-party. Updates and changes to configuration of firewall must be logged by official operators of third-party.
- The **experience and expertise** of the third-party team offering the service of management should be considered by Gingerwood when outsourcing the management of firewall. Gingerwood High School can also install or enable software firewalls on its databases along with the services offered by the third-party to offer an extra protective layer. This may also solve the problem SQL Injection vulnerabilities in case of database security.

4.3. Security of Emails

- “Mail Security Technology” can be implemented to block and detect transmission of malware via electronic mail, in addition to unsolicited mail and other mails intended to threaten students and teachers. These technical way-outs should be retained up-to-date to uphold precise particulars of the techniques, signatures and sources employed by hackers and avoid the malware distribution by electronic mail.
- If an email address or website is recognized as a malware threat or junk mail, it might be included to the blacklist. Likewise, IT personnel should monitor that Internet Service Provider (ISP) has the accurate procedures prepared to decrease the danger to the other local communities.
- IT personnel should also ensure that students and teachers do not put easy PINs to protect electronic mails from intimidations; “brute force” outbreaks are employed by hackers to try accessibility to mail accounts by means of a lists of general PINs, consequently setting difficult PINs may help to make emails safer.

4.4. Additional measures of e-security

Although firewalls are indispensable to safeguard networks of Gingerwood High School from outbreak, there are additional measures that can be adopted to offer a more in-depth and complete provision of security. Such actions might comprise:

- Heuristic Threat Analysis (HTA)
- Penetration Testing
- Intrusion Prevention Systems (IPS) and/or Intrusion Detection Systems (IDS)

The degree to which these kinds of solutions are needed relies on the requirements of security for GHS and its students and teachers, but these services and systems are only of value when they are well-managed and well-configured.

CHAPTER 5

CONCLUSIONS

Cyber-attacks and risk are here, and they are here to stay. No one is immune not even the personnel office of the richest country in the world, nor the server of one of the largest media companies in the world. Given the omnipresence of these massive, damaging attacks, it is also not a surprise that small, underfunded government agencies and school districts throughout the country have experienced similarly deleterious hacks as of late. Despite the fact that cyber risks are here to stay, they can be managed if the proper steps are taken, which begins with security protocols and increased awareness of this topic. As mentioned throughout this paper, it is imperative that Gingerwood High School focus on providing its own equipment with security parameters established (firewalls, admin passcodes, etc.) or require the individual to bring their own device, which is cost-effective and more secure. As curious pupils are looking to expand their intelligence and capabilities, though it may come with serious consequences, this type of innovation should be fostered and channeled, not hindered. If the student is able to bring their own device, or use a device specified to them by the school, they will not be able to maliciously or mischievously hack into the network. In addition, the students should be educated about cyber security, exploitation and its consequences, as well as the benefits behind understanding what a computer can do to defend off malicious hackers, opposed to contributing to them.

In addition to the need to implement a BYOD policy and educating students, this paper has explored in depth the magnitude of the current cyber-attack threat may exist in GHS and other high schools. As elucidated in the case study of Gingerwood High School, there is a multitude of access points that hackers can gain access to a school’s server and wreak havoc by obtaining confidential information. As well, the forms these access points take continue to grow and vary. They may include the computerized security apparatus used to protect students, the centralized computer network available that connects teachers together within a school, and the new applications (employed by the teachers) to engage students. Also, the computerized security apparatus can protect the newly computerized standardized tests, the databases that contain personal information for educators and students, and the large amounts of money held by schools to operate.

As discussed, these danger points pose severe threats to students and teachers, because if hackers had malicious intent, they could use the information available in schools' computers to commit identity theft, pose physical harm to students, disrupt educational activity, or steal money from the academic institutions themselves. However, despite the gravity of the situation plaguing public schools today, there aren't many realistic policy approaches to fixing this issue. Also, these institutions have limited ability to ensure faculty and student safety without the means of financial support for a cyber-security framework. Although the best fixes would include increased funding from federal and state governments, such policy changes seem to be the most unrealistic, given today's polarized political milieu, especially as it concerns public financing and education.

Rather, policy changes that would make a difference include the consideration of cyber security preparedness in annual audits, partnerships between private schools and public schools, and increased federal grants from the federal government (that don't need congressional approval) that are directed solely towards helping schools bulk up their cyber security. These policy changes would help ameliorate some of the dangers that currently exist, although, without a more serious push to increase funding for schools, these approaches will truly just be nipping at the edges.

It is hard to find a more deserving cause than education in this country yet cyber security remains immersed in the abstract for many Americans who are unable to conceptualize the real risks associated with the increased use of technology in the classroom. Perhaps, as the rate of attacks on public schools increases more will become aware of the dangers that exist, and therefore, more will be done to protect our nation’s most vulnerable citizens. In the meantime, perhaps some of the recommendations noted here will help.

References

Advanced Cyber Threats in State and Local Government. (2014).

Alao, M. (2013). Public School Governance and Cyber Security: School Districts Provide Easy Targets for Cyber Thieves.

Bell, C. (2013, February 25). Hackers empty $900K bank account. Retrieved August 14, 2015.

CRITICAL INFRASTRUCTURE PROTECTION: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology. (2014). Retrieved August 14, 2015.

Chang, R., & Lindelof, B. (2015, May 15). 3 Dixon High students accused of school computer hack. Retrieved August 18, 2015, fromhttp://www.sacbee.com/news/local/crime/article21082899.html

Costrell, R. (2015, July 20). School Pension Costs Have Doubled over the Last Decade, Now Top $1,000 Per Pupil Nationally. Retrieved August 14, 2015.

Dougherty, C. (2014, July 8). Banks Dreading Computer Hacks Call for Cyber War Council. Retrieved August 14, 2015.

Dumas, M. (2015, April 23). Cyber attacks, like those on Sony Pictures and Target, hit Mobile County schools. Retrieved August 18, 2015, fromhttp://www.al.com/news/mobile/index.ssf/2015/04/cyber_attacks_like_those_on_so.html

Fast Facts. (2014). Retrieved August 15, 2015.

Fox. (2008, Apr 16). Same Password for Everything? Not a Good Idea. Retrieved from Fox News: http://www.foxnews.com/story/2008/04/16/same-password-for-everything-not-good-idea.html

HOMELAND SECURITY GRANT PROGRAM, SUPPLEMENTAL RESOURCE: CYBER SECURITY GUIDANCE. (2014). Retrieved August 13, 2015.

Klein, D., Roffi, A., & Hehir, J. (2015, April 2). Cybersecurity and Schools: A Learning Opportunity. Retrieved August 14, 2015.

Lestch, C. (2015, July 19). Cybersecurity in K-12 education: Schools face increased risk of cyber attacks. Retrieved August 18, 2015, from http://fedscoop.com/cybersecurity-in-k-12-education-schools-around-the-country-face-risk-of-cyber-attacks

McDonald, T. (2014, June 12). Jersey City school district is probing apparent data breach involving students' personal info. Retrieved August 18, 2015, fro http://www.nj.com/hudson/index.ssf/2014/06/jersey_city_school_district_looking_into_possible_security_breach_involving_students_personal_info.html

Meehan, S. (2013, September 23). Cyber Attacks on School Networks Increasing. Retrieved August 18, 2015, fromhttp://blogs.edweek.org/edweek/DigitalEducation/2013/09/cyber_attacks_on_school_networ.html

Murray, P. (2015, June 22). NATIONAL: CONCERN OVER GOVT CYBER ATTACKS. Retrieved August 14, 2015, fromhttp://www.monmouth.edu/assets/0/32212254770/32212254991/32212254992/32212254994/32212254995/30064771087/3286478c-fe28-4e78-9183-f402125375fb.pdf

Nasr, A. (2015, July 7). Cyberattacks Behind Terrorism on List of Biggest Threats to U.S., Voters Say - Morning Consult. Retrieved August 13, 2015.

National Infrastructure Protection Plan. (2015, June 16). Retrieved August 13, 2015.

Proposed S.3898 Amendment to the Electronic Fund Transfer Act Would Shift Risk of Loss to Banks. (2010, October 13). Retrieved August 18, 2015, fromhttp://www.infolawgroup.com/2010/10/articles/efta/proposed-s3898-amendment-to-the-electronic-fund-transfer-act-would-shift-risk-of-loss-to-banks/

Rainie, L., Anderson, J., & Connolly, J. (2014, October 29). Cyber Attacks Likely to Increase. Retrieved August 14, 2015.

Ranger, S. (2013, Dec 18). There are 18.5 million software developers in the world – but which country has the most? Retrieved from Tech Republic: http://www.techrepublic.com/blog/european-technology/there-are-185-million-software-developers-in-the-world-but-which-country-has-the-most/

Rodriguez, E. (2015, March 9). State Investigating Cyber-Attack on FSA Testing System. Retrieved August 18, 2015, from http://miami.cbslocal.com/2015/03/09/state-investigating-cyber-attack-on-fsa-testing-system/

Rosario, F., Calabrese, E., & O'Neill, N. (2015, February 27). Teen accused of hacking high school, improving grades. Retrieved August 18, 2015, from http://nypost.com/2015/02/27/cyber-hacking-si-student-changed-grades-from-his-smartphone-cops/

Sanburn, J. (2012, July 3). How Exactly Do Cyber Criminals Steal $78, Million? Retrieved August 14, 2015.

Scott, T. (2015, July 31). Strengthening & Enhancing Federal Cybersecurity for the 21st Century. Retrieved August 13, 2015, fromhttps://www.whitehouse.gov/blog/2015/07/31/strengthening-enhancing-federal-cybersecurity-21st-century

Stringcanteam. Several Common Ways that Network Viruses Spread. (2015, February 24). Retrieved August 14, 2015.

Stabley, M. (2010, January 30). High School Students Suspected of Hacking, Changing Grades. Retrieved August 13, 2015, from http://www.nbcwashington.com/news/local/High-School-Students-Suspected-of-Hacking-Changing-Grades-82998367.html

The World's Most Valuable Brands. (n.d.). Retrieved August 14, 2015.

The history of cyber attacks - a timeline. (n.d.). Retrieved August 15, 2015, from http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

US Census Bureau, E. (2015, June 1). Public Education Finances: 2013. Retrieved August 13, 2015.

Whelan, C. (2015, March 11). Public School Extracurricular Program Fights Threat Of Cyberattacks. Retrieved August 14, 2015, from http://losangeles.cbslocal.com/2015/03/11/public-school-extracurricular-program-fights-threat-of-cyberattacks/