8-2021

INVESTIGATING THE RANSOMWARE INFECTION RATE OF K12 SCHOOL DISTRICTS DURING THE COVID PANDEMIC

Gil Abraham Lopez

INVESTIGATING THE RANSOMWARE INFECTION RATE OF K12 SCHOOL DISTRICTS DURING THE COVID PANDEMIC

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology

by

Gil Abraham Lopez

August 2021

INVESTIGATING THE RANSOMWARE INFECTION RATE OF K12 SCHOOL DISTRICTS DURING THE COVID PANDEMIC

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Gil Abraham Lopez

August 2021

Approved by:

Dr. Conrad Shayo, Committee, Chair

Denise Kinsey, Committee Member

Javad Varzandeh PhD, Department Chair

ABSTRACT

Ransomware attacks have become part of the normal vernacular, as more organizations get attacked and must deal with the outcome in the media. School districts are in a unique position because of COVID and the sudden shift to online or hybrid learning. Over the past few years, ransomware attacks on K12 school districts have been widely reported in the news, leading to questions on whether K12 school districts are more vulnerable to these attacks. This project focused on: the prevalence of ransomware attacks in K12 School Districts in the USA in general and in the Inland Empire in particular, examining what value attackers gain by attacking a school district as well as looking at the costs incurred to the district because of an attack, whether K12 School districts in the Inland Empire are following cybersecurity best practices to protect in case of a ransomware attack. The findings are: that school districts are at a higher risk of ransomware attacks because they are soft targets with understaffed under budgeted IT departments, school districts do not pay ransoms and are left with the higher cost or remediation, there is a lack of security focus in the job descriptions for IT managers working in K12 in the Inland Empire, temporary school shutdowns due to ransomware are shown to negatively affect the GDP in the long term. The recommendations are: school districts should use COVID relief funds to hire/contract a CISO and figure out a way to keep the position funded into the future, school districts in the Inland Empire should hire more IT staff and focus on security awareness training for its users including students, schools should move

away from passwords and replace it with 2FA using badge and pins. For future study the issues of long term funding for CISO positions and the creation of security awareness for K12 students needs to be addressed.

ACKNOWLEDGEMENTS

I want to thank my wife Veronica for supporting me while I worked on this project. This is also for my parents who always encouraged and supported me to go to school and follow my interests. I love you all with all my heart.

I would also like to thank Professor Conrad Shayo and Denise Kinsey for guiding me throughout this project.

TABLE OF CONTENTS

ABSTRACT iii

ACKNOWLEDGEMENTS v

LIST OF FIGURES viii

CHAPTER ONE: INTRODUCTION TO RANSOMWARE 1

What is Ransomware 1

How Ransomware Affects K12 School Districts Information System 4

Problem Statement 6

CHAPTER TWO: EVALUATING K12 INFORMATION SYSTEMS 10

How K12 Information Systems are Setup 10

Staff and Student Involvement in the Information System 10

K12 Information System Policies 14

Data Flow In and Out 17

CHAPTER THREE: THE RISK OF RANSOMWARE IN K12 SCHOOL 20

Assessing Vulnerability in K12 Information Systems 20

Evaluating Entry Points for Ransomware 23

CHAPTER FOUR: ANALYZING ATTACKS ON K12 SCHOOLS 28

Ransomware Attacks on the Rise 28

Fiscal Impact 28

Impact on Student Learning 32

CHAPTER FIVE: PLANS FOR DEALING WITH MALWARE 34

Conclusion 34

APPENDIX A: AVERAGE DAILY ATTENDANCE COMPENSATION 44

APPENDIX B: DISTRICTS WITH CHIEF INFORMATION SECURITY OFFICER POSITIONS 46

APPENDIX C: COMMON PORTS 49

APPENDIX D: RANSOMWARE DATA 2019 – 2020 51

REFERENCES 53

LIST OF FIGURES

Figure 1. Student System Components (Lopez, 2021)..……11

Figure 2. Porn Consumption Under 18 (Warner, 2017)……..…..……..14

Figure 3. Vulnerability Targets……..……..21

CHAPTER ONE

INTRODUCTION TO RANSOMWARE

What is Ransomware?

Ransomware is designed to encrypt a user's data and then ask for money in return for a key to unlock the data. The process has become much more sophisticated than this with automated processes that handle the infection, encryption of files, generation of a ransom file, and handling of encryption keys (O'Kane, 2018). Ransomware can infect any device or operating system. It can also encrypt an entire system or hard drive, causing it to become non-operational (Liska, 2017).

The first ransomware ever created was called AIDS, and it was developed by Dr. Joseph Popp in 1989 (Ipsen, 2021). It is uncertain as to why he created the ransomware, since he was later prosecuted for distributing AIDS but found unfit for trial by reason of insanity (Ipsen, 2021). Popp chose to distribute the ransomware via floppy at a World Health Organization AIDS conference (Ipsen, 2021). Users would load the floppy disk into their computers and, when launched, it would replace an AUTOEXEC.EXE file and wait for the system to be rebooted 90 times (Ipsen, 2021). On the 90th startup, it would encrypt the file names using symmetrical key encryption (Ipsen, 2021). The ransom demanded was $189, which needed to be sent to the PC Cyborg Corporation PO BOX in Panama (Ipsen, 2021). A group of researchers later developed a decryption utility called AIDSOUT that would decrypt the files.

Cryptocurrency, as ransomware payment, also gave rise to the popularity of being able to set up a payment network without having a way for it to be traced back to the hacker. Bitcoin specifically accounts for up to 98% of all ransomware payments (JARETH, 2019). Bitcoin's original purpose, as described by the organization’s website, is to create a consensus payment network that is completely digital, decentralized, peer-to-peer, and powered by the users with no middlemen (Frequently Asked Questions, 2021). This decentralized nature allows hackers to request and accept payment with Bitcoin and not have to worry about being tracked. Hackers also use services like mycryptomixer.com as a crypto tumbler that further anonymizes the hacker from the ransomware payment so they can convert and spend it using a fiat currency (Bitcoin Mixer, 2021).

Modern ransomware operates with the business model of creating a problem and a potential solution (as some ransoms are paid and no key is provided). Hackers are interested in getting paid for the decryption key. This creates an incentive for them to provide the decryption key, since not providing it will decrease the confidence that people have in these hackers. If hackers create a reputation for not sending a decryption key, then there will be a decrease in individuals who are willing to pay due to a lack of confidence (Michael Schwirtz, 2021).

Ransomware operators must provide some level of customer service to those they infect. An example of this customer service is when a woman who, using her encrypted laptop, encountered difficulty in purchasing Bitcoins needed

to pay the ransom. She was able to communicate with the hackers who let her get away with underpaying the $500 ransom and still provide the decryption program (Studios, 2015). The majority of people have still never bought or used any crypto currency, and it can be a steep learning curve if your first transaction is for the purposes of paying a ransom (NASDAQ, 2021).

It is estimated that $20 billion in ransomware payments will be made in 2021 (Morgan, 2021). The first iterations of the ransomware Wannacry used an unpatched exploit in the Server Message Block (SMB) protocol to scan and replicate itself over ports 139 and 445 (APPENDIX C). After infecting a system, it would install a backdoor tool called DoublePulsar that allowed persistent access (Martin Lee, 2017). Next, it would scan the internal network and any external networks that it had access to. With each file that it encrypted, it would generate an executable that would pop up with instructions on how to buy Bitcoins and where to send them in return for the decryption program. Patching the SMB bug was the only way to avoid infection.

The future for ransomware will be to follow the general trend in IT, which is to move to the cloud. The target for ransomware has been local systems that are not properly backed up (Galov, 2021). Continuing the trend of businesses moving to the cloud, a new breed of ransomware will be developed to target cloud hosted services. Individual businesses using the cloud can limit the damage done by ransomware in the cloud by developing apps that are cloud host agnostic. This

allows moving to another hosting provider with minimal effort. Data should also be backed up and follow the 3 versions in 3 locations on 2 mediums strategy.

How Ransomware Affects K12 School Districts Information System

Ransomware directly affects schools by encrypting files or drives and not allowing any staff or students access to those files. Ransomware averages around 3 seconds to begin encrypting files on a computer once it infects the machine (Arctic Wolf Networks, Inc., 2016). With this speed of infection, leaving a computer turned on overnight would cause it to have all its files encrypted by morning. Some security advisors advocate for turning off your computer at night to slow and stop the spread of a ransomware attack (Panda Security, 2020).

Leaving a computer turned off at night might slow down the infection rate on a local machine. The reality is that it would not likely make a dramatic difference since most files are stored on a Network Attached Storage device (NAS) that contains the files of hundreds of potentially individuals. Storing files on a NAS is one way to store and more easily backup users' files. Another advantage of storing users files on a NAS is that it allows the user to access their files from multiple computers since they only need to connect to the network to retrieve their files. This is preferable to storing and backing up files on a local machine. Instead of having to install and manage a backup for every machine that a user might use, they can instead configure backups of the NAS and thus be able to back up hundreds of users' files at once.

The policy on Windows environments that allows access to users files from multiple computers is called folder redirection. It is configured through a domain controller's group policy (Deploy Folder Redirection with Offline Files, 2021). When setting up folder redirection of the users' documents to a Windows File Server, it is important that the correct permissions are set for users. If set up correctly then only the user will have access to the files in the redirected folder on the file server. An administrator can access these folders at any time from the file server as a domain administrator, but they run the risk of changing the folder's permission and allowing more access to the files than needed if the policy is not correctly set up (Microsoft, 2008).

If the files are only accessible by the directory user, then in the case of a ransomware attack only the files they have access to can be encrypted. For this reason, it is important that folder redirection be configured with limited rights that allow only the logged in user access. Incorrectly setting folder permissions can lead to the ransomware encrypting more files than it would have originally. This can escalate to the entire file server getting encrypted if the account that is compromised has administrative rights and access to all the files. An administrative account may have access to the file servers and to other infrastructure servers providing services like DHCP, DNS, Active Directory, and vendor specific servers.

When ransomware targets Active Directory, it has access to all the information required for users to authenticate across the network. One example

where this type of attack took place is Norsk Hydro. One employee unknowingly opened a malicious email on a trusted computer three months prior to the ransomware demand (Briggs, 2019). From the time the email was opened to when the attack took place, the hackers planned and used Active Directory to push out the attack using the domain controller (Briggs, 2019). Since the domain controller has an administrative trust relationship with all machines and users on the domain, its spread is almost unstoppable once infected.

Many school districts rely on services like folder redirection and active directory. If the servers hosting these services become infected with ransomware, it would render users unable to use Active Directory for user authentication or to load their files with folder redirection. This would also cause a cascading effect on other services that use Active Directory for account creation and synchronization, like Google Cloud Directory Sync and Google Password Sync. The Google services may continue to run, but without Active Directory new accounts and password changes would require manual updates. It should be noted that some schools that use Chromebooks for all students and staff are so far safe from ransomware attacks. Some school districts that are shutdown from ransomware will often continue to be able to use their Chromebooks (OXENDEN, 2020).

Problem Statement

This project investigates whether K12 school districts in the USA in general and in the Inland Empire in particular are more likely to experience a

ransomware attack when compared to government institutions or businesses. The focus is on the following questions:

- Is there data to suggest ransomware attacks are targeting school districts in the USA?
- Are K12 school districts in the Inland Empire following best practices to avoid ransomware attacks?
- What are the cost implications to ransomware attacks on a cost and loss of instructional time for students?

Information was collected to compare the amount of ransomware attacks that have affected K12 school districts for the 2020 - 2021 school year (see APPENDIX D). This was compared to information available from other government agencies and businesses. Comparing the attack rates should allow for a conclusion to be drawn on whether ransomware is targeting K12 school districts, fall in line, or are less when compared to other government agencies or businesses in the USA and specifically in the Inland Empire (San Bernardino and Riverside Counties)..

Focus was on how K12 school districts configured their information systems and how they structured and trained their employees to be cybersecurity aware and guard against cyber attacks. Checking to see if there are training manuals or training provided that details how internal employees should deal with possible ransomware attacks will show if they are prepared for a possible attack.

District websites were checked to see if they linked to internal resources that could be targeted.

Next, an analysis was conducted on the information services departments at K12 school districts to identify best practices that will aid in avoiding ransomware infections. Emphasis was placed on prevention methods that are specific to K12 school districts. Examples of how some Inland Empire K12 school district information technology departments structure their systems will be given and suggestions made on how to best secure them from being infected with ransomware.

It was also important to look at what the cost was for a district that experienced a ransomware attack. We will look at available articles that detail any additional costs that were incurred because of a ransomware attack. School districts also include contract items in the monthly or weekly board meetings. This necessitates examining board meeting minutes and agendas to see if there are cost items associated with services purchased that could be related to ransomware mitigation or remediation.

I also relied on my 7 years of IT experience having worked at four school districts in the Inland Empire and High Desert communities. My roles included classified titles like Computer Technician and Systems Application Specialist, to the most current management position of Data Warehouse Administrator.

This project was organized as follows: Chapter 2 evaluated K-12 Information Systems, Chapter 3 examines the risk of ransomware in K-12 school

districts, Chapter 4 analyses the attacks on K-12 Schools, and Chapter 5 is the conclusion.

CHAPTER TWO

EVALUATING K12 INFORMATION SYSTEMS

How K12 Information Systems are Setup

All school districts' information services are set up in very similar ways due to lucrative discounts from Microsoft (CITE, 2021) and Google Workspace (Google, 2021). They have a student information system (SIS) that is provided by a third party. School staff enter data to the SIS for student/staff demographics, generating schedules, program information, etc. Staff and student directory accounts exist for accessing various internal or external systems. There is a private network that connects all of these systems together and provides access to the internet. There are local and state reporting agencies that track staff and student data within the system. Between all these systems is the flow of data that is generated by everyone using the system to track student items including progress, behavior, and academic milestones.

The SIS is the heart of the school district's data. It contains the following information: student demographics, staff assignments, class schedules, student behavior data, special program data, and much more. Data entry into the SIS occurs on a constant basis throughout the year and most of the certificated staff are the ones primarily doing the data entry. Certificated staff use the data to create reports and make decisions based on these reports.

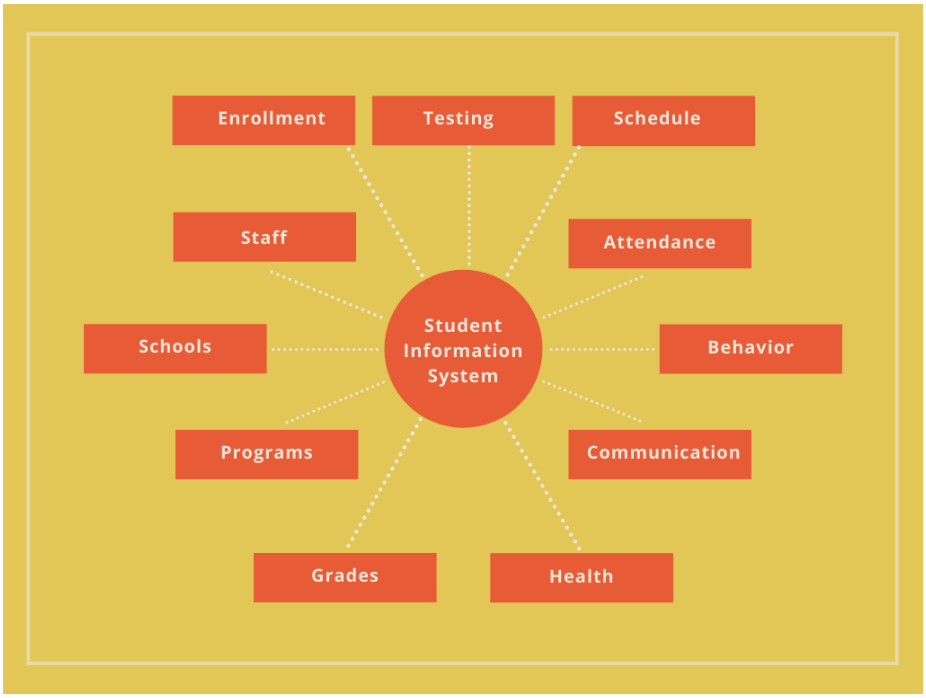

Figure 1 Student System Components (Lopez, 2021).

User Accounts are created from the SIS or through a combination of another system and the SIS. Human resources may have additional systems where staff information is first entered during a pre-hire stage. Through the use of one of these systems staff and student accounts are created. Identity management in the education space is dominated by Microsoft Active Directory and Google Workspace for education (Cavanagh, 2017). Other alternatives such as Clever or One Roster exist, but those usually receive data from the SIS or Active Directory or Google Workspace.

Single Sign On (SSO) has been popularized because of Google Workspace, Microsoft Azure AD, Classlink, and Clever across many learning

platforms online. Using the credentials from one identity provider allows users to not have to memorize multiple logins for different websites. Properly implemented SSO has had the overall effect of making the identity logins of a user more secure because the user is able to create one stronger password rather than having to use different ones across multiple identities. (Sciarretta, 2017). Not all applications can be converted to use SSO, but it is one of the biggest factors when purchasing new online curriculum programs because users do not need to learn a new login method (Gellert, 2017).

The network for a K12 school district can vary widely due to geographical constraints. Most school districts in California are connected via private fiber and are interconnected through the K12 High Speed Network (California K-12 High Speed Network, 2021). Districts such as the Ontario-Montclair School District inner connect their school networks through redundant fiber links between school sites (District, 2017). One forced change due to COVID-19 for some school districts that were still in the planning stages is the reliance on laptops for teachers and students.

Depending on the resource used by students, the need for them to connect into the district network may not exist. Any internal resources like file servers or applications would require a VPN or remote-control connection to an internal system. Another alternative would be to replace or migrate internal services to the cloud. Software as a Service (SaaS) has become a way to move some of the burden from inside the datacenter to the application vendor's cloud

infrastructure. Moving systems to the cloud requires planning for downtime and data migration, this would all have to be expedited to allow for the rapid change to distance learning.

Staff and Student Involvement in the Information System

Systems within a K12 school district get used by school staff, students, and even parents. Pre-COVID-19 students would typically only interact with the computer systems while physically present in the school classroom. Post-COVID-19 it is likely that the students will engage in a model where the device travels with the student back home. This is a newer model for student devices (Herold, 2020). District devices for staff have traditionally traveled back and forth if they were mobile devices.

More mobile devices used mobily means there is a higher chance of devices getting misplaced or stolen when compared to a stationary desktop. If a mobile device ends up in the wrong hands, then it can be used as an infection tool for a malicious actor. A more likely scenario though, is that the device will connect to a less secure home network that does not have as much security as a school district network. Studies show that a home network is up to 3.5 times more likely to contain at least one device with malware (DAHLBERG, 2020). With the amount of device movement from the home into the school district, there is a higher risk of infection from outside the network than from within.

Students who may be less technologically literate, or more willing to click on untrustworthy websites when searching, may encounter ransomware more

than staff. Younger children when given access to technology they may not have had before are likely to search for pornography. A study that researched if top porn sites had more malware than other websites concluded that they did in fact have higher rates of hosted malware (Top porn sites lead to malware, 2013). Malware on these top porn sites would linger in the advertisements that were provided from third party ad networks.

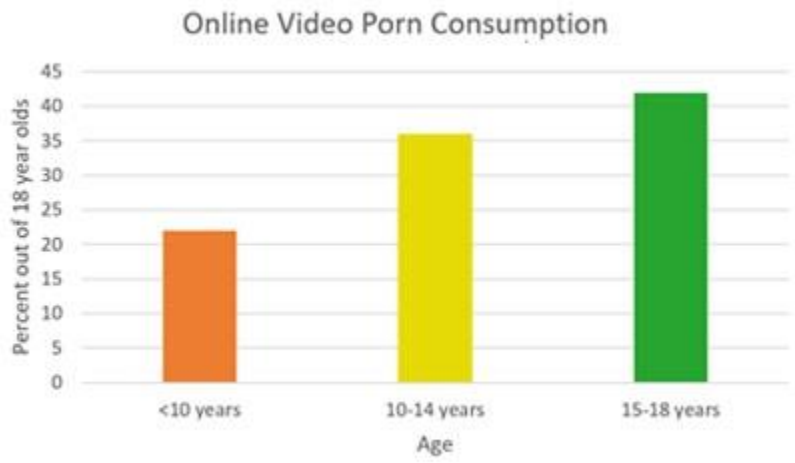

Figure 2 Porn Consumption Under 18 (Warner, 2017)

K12 Information System Policies.

End user training to reduce ransomware infections has become more common in the K12 education sector thanks to E-Rate funding from the

government. For the 2021 school year, E-Rate funding set a spending cap of $4.276 billion dollars(Consumer and Governmental Affairs, 2021). In a survey studying the cost of cybersecurity across 65 school districts, it was found that all had some form of end user training(Networking, 2018). This compares to 95% of executives at businesses, law enforcement services and government agencies who stated their employees receive security awareness training at least once per year (Liu, 2018). The rigor of the training included active end-user phishing awareness with simulated phishing attacks and cybersecurity awareness training. This training was however mostly optional since there is limited time for staff to participate because they are also expected to participate in other mandatory training. In the three school districts where I have worked the last five years, all incorporated some form of training to detect phishing attacks over the web and email.

Password policies are difficult to implement because users are affected by the already growing list of passwords that they must remember. NIST security standards suggest the following (NIST, 2017):

- A password must be changed at least every 60 days.
- Prevent users from selecting previously used passwords.
- Check passwords against a list of weak passwords.
- Set complexity requirements that specify the minimum number of characters and that a mix of character types be used.

These password recommendations typically result in backlash from users because it is a task that often stops them from doing their job and requires additional work from them.

Physical security is sometimes overlooked since it may be the last thing that management would expect to be compromised. Limiting access to infrastructure like servers in a datacenter by having specific keys for the entrance door or using a RFID scanner to allow access should be a base-level of physical security for the infrastructure. This would discourage normal day to day employees from entering the room and require that visitors contact someone with the appropriate access to validate their need for temporary access.

Other physical security would be encouraging staff to lock their computers when walking away from their desk. Pairing this information with a screensaver policy that requires a password to unlock the computer is recommended by the NIST, PCI DSS, an ISO 27001 (DeMeyer, 2019). Having no lockout policy means that anyone walking by can have access to your system and can browse with the logged in users' permissions. This policy would stop from leaving a system open if a simple break turns into a weekend of unlocked computer access for anyone to use.

Password sharing has been a solution for teachers and staff to give access to a substitute while they are out. For Example, teachers would share their password on a sticky note or let the front office know what the password was when they were out (Amy, 2015). There are many documented cases of

students obtaining the teacher's password due to leaving it on a sticky note and performing activities such as changing their grades (LEAL, 2009). This method to provide access to substitutes has been curbed by the fact that SSO would give the substitute access to the teachers email and other systems.

Data Flow In and Out

School districts rely on third party online or digital curriculum vendors to aid teachers in educating students. Online curriculum vendors need tsystem access to create accounts for students and staff. Sending .txt, .csv, or excel files to an FTP or SFTP server has been a standard option for many years. It allows for data export from the SIS, organizes it into a file, and sends it over in an automated way. This process can become unmanageable since more digital curriculums lead to more data uploads that require more management. The growing trend has been to use a SSO provider like Clever or Class link to simplify adding new curriculum vendors.

They centralize sharing data to third party curriculum vendors through rules that are setup on their web portal. To do this they require a district to send a complete roster of all their students, staff, schools, classes, and teachers to Clever nightly. This data is integrated and from there you can select from the approved list of third party integrations to quickly share this roistering information and set an approved set of students.

School districts are also incrementally moving to the cloud to ease on management and cost of upgrades to existing infrastructure. From 2014 to 2016,

400 school districts surveyed moved from providing 42% of their IT solutions fully or partially in the cloud to 74% (CDW, 2016). The service that migrated from hosted to the cloud the most was email which moved from 64% to 88% fully hosted during that period. Other services which have seen partial migration to the cloud include SQL due to the ability to provide redundancy, scalability, and backup. Licensing costs for Microsoft SQL are often more expensive than the initial cost of moving it to the cloud. This along with not wanting to fully commit to hosting critical infrastructure services in the cloud is a reason why many schools choose to keep copies of their data in the cloud (Bertram, 2016).

Cloud hosted email platforms like Office 365 and Google Workspace contain much of the data that an organization creates daily. Email and file storage are two areas where these platforms get used by all users in the district. Some of the data that is shared to county and state agencies is student medical data.

Medical data is collected for students on an ongoing basis. This information can include events such as visits to the nurse's office due to run-of-the-mill illness or minor injuries. Other patient data contains more sensitive medical history that can include a student's mental health. There are many ways the data can be harvested for a ransom that would greatly damage the district due to the Health Insurance Portability and Accountability Act (HIPAA) or other financial violations if it were to be released(American Medical Association, 2021). This is one of the items that hackers use to bargain with the compromised school

districts if they resist paying the ransom. While the information may have limited value to the hackers, it can expose the school district to a high amount of financial responsibility if it were leaked.

CHAPTER THREE

THE RISK OF RANSOMWARE IN K12 SCHOOLS

Schools may not have instruction available year-round, but that does not mean that the schools remain empty, and that technology is not in use year-round. Office staff remain at different sites working and are still targeted by ransomware. School districts remain a large and lucrative target according to the security firm Bit Sight (Floeell, 2017). It is estimated that 13% of educational institutions have faced some sort of ransomware infection (Floeell, 2017).

Assessing Vulnerability in K12 Information Systems

The IT staff to student ratio is too large when compared to the best practices set forth in the private sector of 1:82 (Livy, 2018). When students are considered into the overall ratio, the best school district in the Inland Empire has an IT staff to user ratio of 1:603 (APPENDIX B). While more resources are available to IT staff to manage more devices from a central location like Google Workspace, the time needed to properly address basic user needs is not there. High IT staff to user ratios show that there is an over reliance on management tools to attempt to meet the security needs of a district. Understaffing to this degree is identified as a threat to Cybersecurity at a local government level (Caruson, 2012).

Type of Vulnerability	How often targeted	Source
Staff ratios	High	APPENDIX B
Possession of valid user credentials	Medium-High	Verizon, 2021
Unpatched servers or network equipment	Medium-High	Ponemon Institute, 2019
Use system or domain account	Medium-High	Schwartz, 2019
Reinfection of systems	Low-Medium	NCCIC,2016

Figure 3 Vulnerability Targets

It is difficult to attract and maintain the most highly skilled cybersecurity staff that you would rely on to lead cybersecurity initiatives since compensation is better in the private sector (Cole, 2020). Having a high amount of staff turnover because your best cybersecurity staff is constantly rotating out leads to a patchwork of security policies that get implemented, but not updated and maintained (Johnson, 2018). There are other solutions that can be implemented if there is a lack of funds to hire full time cybersecurity staff. These solutions are discussed later in the conclusion..

Laptops require the use of wireless internet to connect to the network. This is provided by home or district Wi-Fi, or with 4g hotspots provided by the school district. Devices that were once connected to only the school networks and had their traffic filtered through a firewall now rely on home networks and mobile broadband vendors to provide a safe connection. Staff devices used to be the only ones moving from an outside network back to the district network, but

now some school districts are offering a blended learning model. This blended learning model allows students some in person and online instruction with their device (Dupree, 2021)..

Policies for devices, firewall, anti-virus and operating systems had to be updated to accommodate for students and staff moving the classroom and office to their homes. The firewall became unable to stop threats at the perimeter because devices were no longer behind it. There were several ways to protect against the threats to the network while still allowing continuity in the classroom and workplace. Two of those methods were to utilize VPN connections to users who needed direct access from their device to the district network, and another was to use remote control software to allow access to other computers inside the network.

Using either of these methods to allow a connection inside the district network meant that new or additional license cost needed to be taken into consideration. VPN clients and remote desktop software (RDS) can be licensed in different ways but being forced to scale up due to COVID meant that costs for IT services went up (Fortune Business Insights, 2020).. Market research shows that overall the annual growth rate of RDS increased 15% from 2019 to 2020. TeamViewer, which provides a RDS solution, had a 75% growth in the first quarter of 2020. Allowing connections into the network meant that the internet connection for the district would be utilized more since those connections no

longer traveled over the local LAN. Overall, IT costs increased for K12 School Districts during the pandemic..

Evaluating Entry Points for Ransomware

Entry points for ransomware are no different from any other virus or malware. Hackers may be targeting a specific company or spamming as many possible targets as possible to see if they can get a hit. Phishing through email spoofing is popular with school districts once the hacker has a list of users' emails available for them to target. The hacker will imitate another user or service to get the victim to either run or open a file attachment, or by sending them to a spoofed website that asks them to login.

Phishing attacks are effective because they get the user to believe in a made-up scenario, such as requiring them to reset their password before it expires or asking them to log into a file hosting site like Microsoft OneDrive or Google Drive to retrieve a file sent to them. When the user logs in, then the hacker can use the credentials they captured to either infiltrate the network. Next, they use the compromised user's access to release ransomware into the district . They may also use the compromised user to send out other spoofed emails to other users with the cover of originating from an actual user. Since hackers spend up to 24 days on average on the network before they infect it with ransomware, they can read the user's emails and create a more specific plan to infect the network (Solutions, 2021).

While the hackers are in possession of valid user credentials, they can use the time they spend on the network to look for other vulnerabilities that present themselves. Unpatched servers or network equipment can be used to gain alternative access points back into the network, or to disable any systems that may detect and remove them. If the hackers can escalate privileges to where they can use system or domain accounts, they can even disable backup systems or modify anti-virus to whitelist their presence.

Other infection methods include remote desktop protocol (RDP) which has been found to be a straightforward way to enter a computer network. This method is used by hackers with commonly available network scanning tools who scan the open internet for open ports 3389 for RDP (APPENDIX C). Once an open RDP port is found, the hacker can run a brute force credential attack (Hail Hydra RDP Brute Force, 2018) that has the credentials for up to 15 billion compromised accounts (Ilascu, 2020).

RDP is a very useful protocol for gaining remote access to computer systems for the purpose of system administration (Microsoft, 2021). Some companies have used RDP on the open web as a free remote access option to systems from outside the network since it only requires an open port on the firewall. RDP can be combined with a VPN to not publicly expose the systems directly to the internet, or a Remote Desktop Gateway can be configured to control access to remote sessions from the outside network to any internal computer.

VPNs have gained a lot of popularity during the pandemic partially because licenses were offered at heavy discounts or free trials of up to 90 days were given (Product Notifications, 2020). VPNs typically operate using a firewall or dedicated VPN server that gets configured to work through the school district's firewall and allows clients to connect to the internal network. There are three main ways that clients can connect to the corporate VPN from their home. One method operates with VPN software that gets installed on the user's device. This allows only the device with the software installed to connect back to the school district's network. A similar option is to use the host operating system's connection profiles to connect to the school district's network. Finally, one method uses a dedicated firewall that has a preconfigured connection to the district network and allows any computer connected to it access through the secure tunnel. This last option allows multiple devices to connect and can even allow wireless devices if the hardware supports Wi-Fi.

An incorrectly configured VPN poses a threat in many ways. An NSA security advisory explains how three different VPN programs provided by three different companies were found to be vulnerable and weaponized by active persistent threat actors (NSA, 2019). The VPN client from Pulse secure had a vulnerability where the attacker could send a specific uniform resource identifier (URI) that would allow arbitrary file reading on the VPN server. This was used to read the configuration files on the VPN proxy server. If SSL was used instead of TLS for securing the VPN gateway, then the ssl_webvpnsession file can be used

to collect the session token, IP Address, Username, and plaintext password of connecting users. An attack like this leads to other exploits that allowed the attacker to write and execute files on the VPN server (Directory traversal, 2020).

Another popular VPN client from Palo Alto Networks had a remote code execution vulnerability that allowed attackers to execute remote code on a VPN gateway that had not been patched (Tsai, 2019). The exploit was rather simple and attacked the SSLMGR by sending a set of parameters for it to execute. One type of parameter request was found to crash the SSL Manager when sent. After crashing the SSL Manager, remote code could be executed to modify certain files. After the files were modified, the SSLMGR became a web console that could be used to execute code.

One final type of VPN exploit that affected Fortinet FortiGate VPN Clients was a backdoor created by the developers. This backdoor was intended to allow for password resets when a user's password had expired. This backdoor served to provide access to the password reset process and it was discovered and exploited by hackers (Tsai, 2019). This backdoor required no authentication if the magic parameter was submitted. The submission required sending a specialized request to the VPN gateway and granted the hacker a console shell that allowed them to set the password for a user. That account could then be used to log into the VPN client and grant network access.

To summarize this chapter, we see that there are staffing and policy issues that cause K12 schools to be vulnerable to ransomware attacks. We also

see that there is proof that hackers are using phishing attacks on staff and that they are scanning for vulnerabilities in VPN and RDS software used by schools because of the pandemic. In the next chapter we will examine how these vulnerabilities and entry points can lead to actual attacks.

CHAPTER FOUR

ANALYZING ATTACKS ON K12 SCHOOLS

Ransomware Attacks on the Rise

According to a report from the K12 Cybersecurity Resource Center, the amount of ransomware attacks increased by 24% with 50 total reported incidents in the US in 2020 (Levin, 2021). Other reports from the CISA state that the ransomware incidents reported to the MS-ISAC from January to July 2020 affected 16% of K12 schools and this number increased to 57% from August to September 2020. They also state that they expect these numbers to rise as school districts continue to rely on distance education for the remainder of the school year (Cybersecurity and Infrastructure Security Agency, 2020).

Fiscal Impact

The individuals and groups that run ransomware operations do it for the financial incentives. Hackers spread ransomware to as many systems as possible while others may spear phish and look for one lucrative company to attack. The end goal for those who spread ransomware is to get paid. To that end, K12 education systems are a different type of target because the amount of financial gain can be limited, but they are also an easier target.

The budget of all K12 school districts in the US is around $760 billion (Levin, 2021).There is one school district who paid a ransom in 2020 of $50,000 to resume opening faster vs taking longer to go through remidiation (Betts, 2020).

The usual ransom requested is $1 million (Levin, 2021). This cost for remediation is on the rise with the average cost for a business to recover from a ransomware attack increasing from $761,106 in 2020 to $1.85 million in 2021 (Ferranti, 2021). Since most school districts opt to not pay the ransom, they are left with the cost and time of recovering from the ransomware attacks.

Overall in 2020 there were 50 reported ransomware attacks that took place in 25 states (Levin, 2021). This is a 24% increase in attacks when compared to 2019. The state with the most attacks during 2020 was Texas with 6 (K-12 SIX, 2021). . There are only 8 states with no reported attacks since 2016, meaning that almost all states have been hit at some point. In the reports and news articles of the attacks, there is no mention of how the malware got onto the networks. School districts are not legally required to provide information on how the ransomware got on to their networks (Department of Homeland Security, 2016).

School closures because of a ransomware attack mean that there may be a loss in the budget that schools collect the following year due to a drop in Average Daily Attendance (ADA). ADA is the primary funding source for school districts in California, and maintaining a high ADA guarantees more funding (Weston, 2010). A decrease in ADA means that the district budget for the next year will be decreased. This can lead to staff being laid off and will result in less programs for students or an increase in student class sizes. Average time for an

organization to recover from a ransomware attack is one to two weeks if an experienced recovery team is involved (Networks, Alvaka, 2021).

Entering data into the SIS is a daily occurrence by numerous staff. If staff were unable to access the SIS for any extended duration of time, it would mean that data normally being entered into the SIS would have to be entered in somewhere else temporarily until the SIS becomes available again. Another consideration is if the SIS were unable for several days during a normal school year, then it may not be possible to keep track of all the changes needed to be made. This can mean that school would have to temporarily be suspended until the SIS can be brought up again, or an alternative data entry method must be put in use. If a temporary data entry method is used, then overtime for data entry staff will likely have to be paid by districts so that the data can be entered into the SIS once it is brought back up online.

There is value in the data housed in the SIS. Health data or student/staff personal identifiable information like birthdays, addresses, and social securities are often stored in the SIS. This data can be sold on the black market if the ransom is paid for or not (MELENDEZ, 2020). It can also cause a fine for violating HIPPA laws if the data were to be released.

Resetting passwords at the beginning of the school year is a common and time-consuming practice. The helpdesk and ticket system are flooded with staff and students who cannot log in because they forgot their password over the summer. A ransomware attack would trigger a mass password reset scenario for

all staff and students. This is required to ensure that if the password database were compromised, that the attackers would not have access to the user's data after systems come back online. The estimated cost of a password reset based on the effort of the help desk personnel is around $70 per reset for larger organizations (Frost, 2017). This cost would not include the time that staff spend resetting passwords and teaching students their new passwords.

Providing staff with security awareness training with the goals of risk reduction of reinfection can cost a considerable amount of money depending on the quality and scope of training. Some estimates for this type of training, which included phishing attacks on all employees, range from $21,600 for 200 staff (The Return On Investment (ROI) of Security Awareness Training, 2019) to an average of $290K for companies with 1,000 to 5,000 employees (Seals, 2017). It is also estimated that employees need around 7 hours of training per year to maintain an up to date level of security awareness(Living Security, 2020).

A ransomware attack may also lead to other costs that stem from a loss of reputation from a cyber-attack. Certain areas of the country are very competitive when it comes to student enrollment since parents can choose what district to enroll into (Kronholz, 2014). Negative media coverage and a poor response from the school district may also play into diminishing the reputation of certain districts. Staff may also experience lowered morale due to loss of files or the added stress and additional workload from dealing with the attack. With the

looming teacher shortage, it may make it more difficult for school districts to attract new teachers (Weiss, 2019).

IT staff specifically may suffer from lower morale that can lower their productivity. This can be more severe if the notices and information given from IT is not taken seriously or followed by the organization's users after a ransomware attack (Myers, 2021).

Teachers may not be the most technically savvy and may not have offline backups of data. This means that in a data loss situation, it is possible for a teacher or staff member to lose years of lesson plans or undocumented data. This will lead to a loss of productivity and reduction in teacher morale since many will likely work unpaid overtime to recreate the lost content (McLoud, 2019).

Impact on Student Learning

The main goal of a school is to serve its community by providing education to its students. Any disruption to that process causes a loss of instructional time. A loss of instructional time can occur if internal systems or processes that students rely on are affected by ransomware. Processes like student account creation or having to shut down a network to stop the spread of ransomware are examples we will explore (Ransomware Attacks on School Districts, 2020).

To simplify student sign on for third party learning software, Single Sign on (SSO) has become a necessity that helps cut down on the time it takes to teach students to sign on to new curriculum websites. A ransomware attack would likely disrupt the process that synchronizes data between the SIS and the SSO

vendor and cause login disruptions for students. Online video conferencing is how class is being conducted during the COVID shutdown and a disruption in synchronizing student accounts would make holding class impossible.

Closing a school and not being able to hold instruction is detrimental to the academic achievement of students. An estimate by the NWEA shows that there was up to a 50% decrease in student learning gains in math when students returned to school after a closure (Tarasawa, 2020). Other reports studying the GDP effects of low student achievement scores, showed that a population with higher achievement scores increased GDP for their country vs those with lower scores (OCED, 2010). Closing schools will likely result in a noticeable statistical change to certain parts of the economy because of ransomware.

CHAPTER FIVE

PLANS FOR DEALING WITH MALWARE

Conclusion

Based on the research I have done on examining 20 different school district positions, staff and student counts, and checking union contracts to see if there is an opportunity for professional development, we see how ransomware affects K12 school districts(APPENDIX B), I make the recommendations below. These recommendations are tailored towards school districts.

Get a Chief Information Security Officer

School districts should bring on a Chief Information Security Officer (CISO) to continuously review their organizations security practices. If the school district is too small, then they can hire one to provide this service for several hours per month. Alternatively, a small district can work with other smaller districts to hire a full-time security manager that fulfills this role. One other option is to work with the county to provide this service for all or some of its school districts under its management. After surveying the job descriptions of 20 school districts in the Inland Empire, I found that only two had dedicated security managers and many did not include the word security in their job descriptions (APPENDIX 2).

The importance of this role is that there needs to be an emphasis on security throughout the district. Many schools' districts place security as part of

the job description for specific elements of that job, but it does not tie together the security for the entire district across different IT areas. One of the roles of a CISO is Governance in an organization (Fruhlinger, 2021). This means making sure all security initiatives are working well and that management knows where their funding is going. Like in other public private sectors, I believe the lack of governance in K12 school districts is what makes them vulnerable to ransomware attacks (GUENTHER, 2019).

With various IT departments focused on their own internal projects it takes a CISO to focus on security for the big picture. An emphasis on a patching schedule for various systems will also increase the overall security of the school district. Patching methodology depends on the person making the decision of when to patch. Past experiences mixed with the risk of financial loss from a patch causing downtime influence these decisions (Rajivan, 2020). With a dedicated CISO there should be more time for testing patches for critical production systems and this will lead to a reduction in the time it takes to patch systems. Patching sooner leads to better overall security (Rajivan, 2020).

For many school districts patching a system when needed is not an issue because the hardware or software is end of life (EOL) and no longer supported (Hennick, 2020). Products that enter the EOL phase pose a security risk to their organization (CISA, 2020). There are several reasons why school districts continue to use systems that are EOL. As of last year, around 20% of a 400 school survey stated that they were delaying upgrading from Windows 7 with no

solid plans to update these systems (Pennell, 2020). Windows 7 went EOL on January 7, 2020 and Microsoft announced that it was stopping extended support for Windows 7 in 2015 (Kelly, 2014). This is just one example where a CISO could work on a plan to move away from EOL software given enough time.

Funding Upgrades After the Pandemic

While there are many downsides to COVID, one positive note for K12 school districts is the additional funding allocated for pandemic relief. Two relief bills were passed by the US Department of Education. The Governor's Emergency Education Relief Fund (GEER) and Elementary and Secondary School Emergency Relief Fund (ESSER). These funds respectively award totals of $4 billion (Governor's Emergency Education Relief Fund, 2020) and $189 billion (Elementary and Secondary School Emergency Relief Fund, 2020) in relief to schools in waves based on a funding formula. This money is available to improve cybersecurity since it will help with the transition to hybrid learning (Frequently Asked Questions, 2021). When the emergency relief funds are no longer available then cuts to other programs will likely have to be made in order to continue to have the CISO position.

Funding from these sources can be used to restructure how personnel and projects get funded. Money that was unavailable for funding much needed IT projects and personnel is now available through federal funding. Alongside hiring a CISO, these new funds can be used to upgrade aging systems that are at or

nearing EOL status. A new approach should be taken when replacing aging systems that incorporate higher security levels and better thought-out policies.

Reviewing past policies and updating them to meet a higher security threshold is also something that the CISO role will take charge of. It is reported that 54% of IT leaders lack the budget to meet the expectations of district management to properly manage their technology (Maylahn, 2015, p. 4). During the period of the survey in the report, it was also reported that budgets were decreasing for 14.9% of the districts surveyed (Maylahn, 2015, p. 21). An IT department with inadequate staffing is likely to make sub optimal policy decisions that favor quick implementations that do not prioritize cybersecurity. Furthermore, it is likely that systems that get implemented are not updated or supported properly since there is not enough staff (Joyce & Nocera, 2021).

One common vulnerability that is affected through policy is the lack of local computer account admin password rotation or variation. For most school districts a common local admin password exists that is not changed and may not meet updated complexity requirements. When using Microsoft's Active Directory, a free local administrator password solution (LAPS) exists that can be configured on the domain to randomize and update the local admin passwords so they are unique for each computer (Microsoft security advisory, 2015). This solution has been around since 2015 yet many school districts have not or were slow to implement it (Haber, 2020). This is often because there is a lack of desire from

level one support staff to have to retrain on a new method to retrieve the local administrator password.

A lack of staff can lead to other issues such as not having enough time to audit existing system security through red and blue team hacking(DeCusatis, 2021). A CISO can direct internal members to find and exploit holes in the existing systems to educate staff on what attacking and defending would look like to an attacker. An approach to securing existing internal systems can have a beneficial effect on overall security because red-blue team exercises help train staff in cybersecurity .

Other valuable information that a CISO could work to protect is the data agreements between a school district and its vendors. Since ransomware operators are known to auction off data, they benefit from the attack whether the ransom is paid or not (Security, 2020). CISO can work with new and existing vendors to specify who owns and controls student and staff data. The data generated and transmitted to third party vendors is not always owned and controlled by the school district. Many third party vendors operate in an opt-out model for sharing student directory information (KIESECKER, 2020). Depending on who is negotiating the contract with the third party vendor, school district administrators can be unaware or ill prepared to ask questions about who owns the data and who has control over it.

Having a contract that clearly states that the school district owns all data uploaded and generated to third party vendors is critical. This contract language

allows the school district to delete their data off third party servers any time, and gives the school district the most control over its data. It is important to hold third party vendors accountable and to have a school district CISO who knows what nuances may exist between the school and third party vendors in case they are compromised.

Another important note with third party vendors, is asking them about the security of their systems to better understand who in the company has access to student data and if the company can be trusted with the data in the first place. Third party vendors can suffer from a lack of security focus when it comes to data and may even be a victim of their own success if they grow too fast. A third party vendor who sells curriculum and online learning materials was infected by ransomware and had parts of its staff and student data accessed by hackers (Paganini, 2020). A CISO could negotiate in a contract the responsibility to be informed when such incidents occur.

Professional Development for students

Since malware attacks are going to be more common in the future because of their profitability, a CISO should work with educators on creating a student curriculum that teaches cybersecurity basics to students. Younger students in elementary school have specifically been identified as higher risk cybersecurity targets (Yan, 2021, p. 9). One specific method for education is direct exposure to cybersecurity situations (Yan, 2021, p. 3). By teaching

students through real world examples, students will develop an aptitude early on for identifying and mitigating cyber attacks on their personal accounts.

Moving Away From Passwords

Passwords are no longer the best way to secure systems that house important and sensitive data. Moving to a new type of authentication method to increase security is an uphill battle since most users are not willing to move away from common passwords (Rome, 2021, p. 75). This remains true even when they are made aware of better more secure methods to authenticate. Employees are overconfident in their company's security and do not see a need to add security until there is a security incident. One reason for the lack of concern from employees, is that they may not see the value of protecting the school districts data since to them the data housed is not of high importance.

Passwords are the weakest link in securing data because hackers are willing to attack specific users through phishing and attack the stored password databases to copy and crack offline (JOSEPH BONNEAU, 2015). The most difficult threat to a password is a targeted phishing attack against one user. These sorts of attacks can be tailored to that user and present the biggest threat. Senior personnel should be required to enroll in multi factor authentication to access email and other important systems. Furthermore, email and other important systems should be selected based on added security features such as suspicious activity checks. When Google added suspicious activity checks to

Gmail that required additional pieces of user data to continue functionality, it decreased hijacking of Gmail accounts by 99.7% (Hearn, 2013).

School districts need to evaluate the SSO providers and internal systems that store passwords to ensure they are hashed and salted so that if the password database is copied to an offline system, it cannot be easily decrypted (LAKE, 2018). Having secure passwords by way of a good password policy that conforms to the NIST Digital identity Guidelines (NIST, 2017) ensures a higher grade of security with better user experience. The guidelines make the following recommendations to be used with multi-factor authentication (Chapple, 2019):

- Password length should be between 8 and 64 characters.
- Disallow new passwords which are identified in a dictionary list of compromised passwords.
- Allow all asci characters and spaces.
- Do not set composition rules.
- Do not expire passwords too often.
- Do not use Knowledge-based Authentication

Emphasis must be placed on combining the above recommendation for staff with some form of non-SMS based multi factor authentication. There are affordable 2FA security tokens from companies like Yubico which start at around $50 (YubiKey 5 Nano, 2021). Alternatively, employees can also set up 2FA using their smartphones and an authenticator app like Microsoft Authenticator

(Microsoft, 2021) or Google Authenticator (Google, 2021). These solutions are all built in and work well with Microsoft Azure Active Directory and Google Workspace for Education. These directory services make up about 94% of the K12 market education market (Mandaro, 2020).

Students should also use 2FA with a badge login for K-2 and badge plus pin for older grades 3-12. This recommendation is based on the research done through Clever and the guidelines that most districts follow closely(Clever.com. 2021). Younger students benefit from a quick login into their devices and programs by using just the badge. There is a physical threat of using a badge, but it is superseded by the fact that student logins are typically written down for grades K-2 anyway. If an attacker gets physical access to any K-2 classroom then they will be able to access the login information of students' whether badges are used or not. Badges persist with the threat that teachers should provide supervision over their classroom and not allow suspicious individuals to rummage through the students' belongings.

Older students should also use badges but add security pins to increase security. Since older students can be more malicious and target other students, the pin serves as an added security measure that can be selected by the individual user. Both major badge login platforms support added pins for grades 7-12, but that can be lowered to Kinder students if desired. These pins and badge act like a 2FA login

Badge logins are offered through multiple companies like Clever and ClassLink and use a generated QR code to allow users to authenticate with any device that has a camera. This works on any Chromebook, iOS or Windows device to allow login into the device and into the OS.

Ransomware will only continue to evolve since it shows no sign of slowing down in companies willing to pay the ransoms. School districts will continue to be targets unless they take their Cybersecurity and professional development seriously.

A further area of study would look into ways of funding the CISO role long term for all school districts. That may as mentioned earlier be a shared cost amongst some schools or counties. Another area to study is the education of students to train them to recognize different types of cyber attacks. Students with this education would benefit society at large since it should aid in preventing attacks wherever they are.

APPENDIX A

AVERAGE DAILY ATTENDANCE COMPENSATION

LEA = Local educational agency	AVG Days in School = 181
EDP 365 = Expenditures for Current Expense of Education	AVG instruction Hours per Day = 6.24

Average by LEA Type Amounts in Dollars

LEA Type	EDP 365	Current Expense ADA	Current Expense Per ADA	Cost per Day	Cost per HR
Elementary	$13,238,607,018.37	$1,046,712.41	$12,647.80	$69.88	$11.20
High	$6,744,321,634.42	$493,224.32	$13,673.94	$75.55	$12.11
Unified	$49,301,984,569.59	$3,683,070.96	$13,386.11	$73.96	$11.85
Statewide	$70,032,149,542.13	$5,278,011.39	$13,268.66	$73.31	$11.75

Average days and instruction time
https://nces.ed.gov/surveys/sass/tables/sass0708_035_s1s.asp

California Cost per ADA
https://www.cde.ca.gov/ds/fd/ec/currentexpense.asp#:~:text=SACS%20Form%20CEA).-,Average%20Daily%20Attendance%20(ADA),the%20total%20days%20of%20instruction.

APPENDIX B

DISTRICTS WITH CHIEF INFORMATION SECURITY OFFICER POSITIONS

District	Has CISO or like position	Security Mentioned in job description	Type	Staff Count	Student Count	Staff to Student Ratio	PD Available
San Bernardino	Y	Y	K12	67	51330	NA	N
Fontana	Y	Y	K12	35	35461	NA	N
Rialto	N	Y	K12	21	24461	1:1165	Y
Colton	N	N	K12	25	20550	1:822	Y
Ontario-Montclair	N	Y	K-8	21	19286	1:918	Y
Jurupa	N	Y	K12	21	18768	1:894	N
Riverside	N	Y	K12	32	40083	1:1253	Y
Moreno Valley	N	Y	K12	26	31597	1:1215	Y
Rim of the World	N	Y	K12	4	2926	1:732	N
Chaffey	N	Y	9-12	20	23854	1:1193	Y
Alta Loma	N	N	K-8	4	5659	1:1415	N
Mt Baldy	N	N	K-8		87	NA	N
Etiwanda	N	N	K-8	11	13478	1:1225	N
Central	N	N	K-8	7	4219	1:603	N
Mountain View	N	Y	K-8	3	2625	1:875	N
Chino	N	Y	K12	26	27333	1:1051	Y
Snowline	N	N	K12	5	7355	1:1471	Y
Hesperia	N	Y	K12	10	24216	1:2422	Y
Yucaipa	N	Y	K12	7	9689	1:1384	N

Corona Norco Unified	N	Y	K12	34	51318	1:1509	Y

APPENDIX C

COMMON PORTS

Protocol	Ports
Server Message Block	139,445
Remote Desktop	3389
Domain Name System	53
Dynamic Host Configuration Protocol	67,68
Lightweight Directory Access Protocol	3389

APPENDIX D

RANSOMWARE DATA 2019 - 2020

Source	Ransomware attacks	Author	Year	URL
The K-12 Cybersecurity Resource Center	50	Douglas A. Levin	2020	https://k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf
The K-12 Cybersecurity Resource Center	37	Douglas A. Levin	2019	https://k12cybersecure.com/wp-content/uploads/2020/03/K12Cybersecurity2019YearinReview.pdf

REFERENCES

American Medical Association. (2021). *HIPAA violations & enforcement*. American Medical Association. https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement

Amy. (2015, April 10). *Substitutes and Class Dojo*. Classroom Tested Resources. https://www.classroomtestedresources.com/2015/04/substitutes-and-classdojo.html

Arctic Wolf Networks, Inc. (2016). *Ransomware infection to encryption in three seconds.* sunnyvale. Arctic Wolf Networks, Inc.

Bertram, A. (2016, February 29). *Cloud-powered SQL gives districts new advantages*. Ed Tech Magazine. https://edtechmagazine.com/k12/article/2016/02/cloud-powered-sql-gives-districts-new-advantages

Betts, M. (2020, July 29). *Athens ISD pays $50K for release of data in ransomware attack*. KETK. https://www.ketk.com/news/education/athens-isd-pays-50k-for-release-of-data-in-ransomware-attack/

Bitcoin Mixer. (2021, June 11). *Frequently asked questions.* MyCrypotoMixer. https://mycryptomixer.com/

Briggs, B. (2019, December 16). *Hackers hit Norsk Hydro with ransomware. The company responded with transparency*. Microsoft Transform. https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

California K-12 High Speed Network. (2021). *Datalink*. K12 HSN Datalink. https://datalink.k12hsn.org/

Caruson, K. M. (2012). Cybersecurity policy-making at the local government level. An analysis of threats, preparedness, and bureaucratic roadblocks to success. *Journal of Homeland Security and Emergency Management*, 9(2), 1-22.

Cavanagh, S. (2017). Amazon, Apple, Google, and Microsoft Battle for K-12 market, and loyalties of educators. *ED Week Market Brief.*

CDW. (2016). *K-12 cloud possibilities. The Journey Continues.* CDW.

Chapple, M. (2019, August 29). Fact or fallacy. stay up to date on the best practices for password security. *Ed Tech Magazine.* https://edtechmagazine.com/k12/article/2019/08/fact-or-fallacy-stay-date-best-practices-password-security

CISA. (2020, 12 10). Cyber actors target K-12 distance learning education to cause disruptions and steal data. *Cybersecurity & Infrastructure Security* Agency. https://us-cert.cisa.gov/ncas/alerts/aa20-345a

CITE. (2021). *CAMSA*. California in IT Education. https://cite.org/page/1_CopyofCAMSA

Clever.com. (2021, Martch 23). *SSO into everything*. Clever. https://clever.com/products/sso

Cole, B. (2020). Preventing ransomware within local government agencies. Electronic Theses, Projects, and Dissertations. 1076, 10-24.

Consumer and Governmental Affairs. (2021, June 21). *E-Rate. Universal service program for schools and libraries.* Federal Communication Commission. https://www.fcc.gov/consumers/guides/universal-service-program-schools-and-libraries-e-rate

Cybersecurity and Infrastructure Security Agency. (2020). Cyber actors target K-12 distance learning education to cause disruptions and steal data. *CISA.*

Dahlberg, D. (2020, April 14). *Identifying unique risks of work from home remote office networks.* Bit Sight. https://www.bitsight.com/blog/identifying-unique-risks-of-work-from-home-remote-office-networks?utm_campaign=press-release&utm_source=press-release&utm_medium=BitSightcom&utm_content=Identifying%20Unique%20Risks%20of%20Work%20from%20Home%20Remote%20Office

DeCusatis, C. B. (2021). Red-blue team exercises for cybersecurity training during a pandemic. IEEE 11th annual computing and communication workshop and conference (p. 1156). *Nevada, USA. IEEE.*

DeMeyer, Z. (2019, December 6). *Understanding policies. Lock Screen*. Jumpcloud. https://jumpcloud.com/blog/policies-lock-screen

Department of Homeland Security. (2016). *Cyber incident feporting. A Unified Message for Reporting to the Federal Government.* https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf

Deploy folder redirection with offline files. (2021, March 12). Microsoft.com. https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/deploy-folder-redirection

Directory traversal. (2020). Port swigger. https://portswigger.net/web-security/file-path-traversal#:~:text=Directory%20traversal%20(also%20known%20as,and%20sensitive%20operating%20system%20files

District, O.-M. S. (2017). Annual organizational meeting of the board of trustees. Ontario-Montclair School District (p. 40). *Ontario. Ontario-Montclair School District.*

Dupree, J. (2021). *Ontario-Montclair School District to begin in-person instruction safely on April 19, 2021.* Ontario. https://www.omsd.net/site/handlers/filedownload.ashx?moduleinstanceid=4392&dataid=20848&FileName=2020-21-08%20In%20Person%20Instruction%20to%20Begin%20April%2019%2020021.pdf

Elementary and Secondary School Emergency Relief Fund. (2020, September 9). Office of Elementary & Secondary Education. https://oese.ed.gov/offices/education-stabilization-fund/elementary-secondary-school-emergency-relief-fund/

Ferranti, M. (2021, May 1). *Ransomware attacks dip, but UAE remediation costs average over $500,000*. CIO. https://www.cio.com/article/3617083/ransomware-costs-decline-in-uae-but-still-average-above-500000.html

Floeell, D. (2017). Schools becoming targets of ransomware. *Communiqué National Association of School Psychologists,* 36.

Fortune Business Insights. (2020, Nov). *Remote desktop software market size, share & COVID-19 impact analysis*. Fortune Business Insights.

https://www.fortunebusinessinsights.com/remote-desktop-software-market-104278

Frequently asked questions. (2021, June 11). Bitcoin.org. 2021

(2021). *Frequently asked questions elementary and secondary school emergency relief programs governor's emergency education relief programs.* Washington, D.C. U.S. Department of Education.

Frost, N. (2017, June 22). *Password management. Getting down to business*. Info Security Group. https://www.infosecurity-magazine.com/webinars/password-management-getting/#:~:text=What's%20more%2C%20passwords%20can%20be,password%20reset%20is%20about%20%2470

Fruhlinger, J. (2021, April 1). *How the CISO role is evolving*. CSO Online. https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html

Galov, N. (2021, January 19). *Cloud adoption statistics for 2021*. https://hostingtribunal.com/: https://hostingtribunal.com/blog/cloud-adoption-statistics/#:~:text=24%25%20rely%20solely%20on%20a,adopt%20cloud%20computing%20by%202020.Nick Galov

George A. Gellert, J. F. (2017). Clinical impact and value of workstation single sign-on. *International Journal of Medical Informatics,* 131-136.

Google. (2021). Google 2-step verification. Google. https://www.google.com/landing/2step/

Google. (2021). *Take your budget further with Google for Education.* Google for Education. https://edu.google.com/promotional-offers/

Governor's Emergency Education Relief Fund. (2020, September 9). Office of Elementary & Secondary Education. https://oese.ed.gov/offices/education-stabilization-fund/governors-emergency-education-relief-fund/

Guenther, W. (2019). *Leveraging board governance for cybersecurity the CISO/CIO perspective.* https://dl.acronis.com/u/rc/WP_Acronis_Cyber_Threats_Report_2020_EN-

US_201201.pdf

Haber, M. J. (2020, January 23). *What does microsoft local administrator password solution really do?.* Beyond Trust. https://www.beyondtrust.com/blog/entry/what-does-microsoft-local-administrator-password-solution-really-do

Hail hydra RDP brute force. (2018, July 24). pwndefend. https://www.pwndefend.com/2018/07/24/hail-hydra-rdp-brute-forcing-with-hydra/

Hearn, M. (2013, February 19). *An update on our war against account hijackers*. Google Security Blog. https://security.googleblog.com/2013/02/an-update-on-our-war-against-account.html

Hennick, C. (2020, July 20). *The value of modernizing the K–12 data center*. Ed Tech Magazine. https://edtechmagazine.com/k12/article/2020/07/value-modernizing-k-12-data-center

Herold, B. (2020, July 23). *Schools handed out millions of digital devices under COVID-19. Now, Thousands Are Missing*. Ed Week. https://www.edweek.org/technology/schools-handed-out-millions-of-digital-devices-under-covid-19-now-thousands-are-missing/2020/07

Ilascu, I. (2020, July 9). *Over 15 billion credentials in circulation on hacker forums*. BleepingComputer. https://www.bleepingcomputer.com/news/security/over-15-billion-credentials-in-circulation-on-hacker-forums/

Ipsen, A. (2021, 03 10). *The cyber resilience blog*. Backup Assist. https://www.backupassist.com/blog/stranger-fiction-origin-ransomware

Jareth. (2019, September 3). *Is ransomware driving up the price of Bitcoin?* EMISOFT. https://blog.emsisoft.com/en/33977/is-ransomware-driving-up-the-price-of-bitcoin/#:~:text=Bitcoin%20accounted%20for%20about%2098,part%20of%20the%20ransomware%20model

Johnson, T. (2018, June 29). *The real problem with tech professionals. High Turnover*. Forbes.

https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2018/06/29/the-real-problem-with-tech-professionals-high-turnover/?sh=4b3404c64201

Joseph Bonneau, C. H. (2015). Theory on passwords has lagged practice, where large providers use back-end smarts to survive with imperfect technology. *Communication of the ACM*, 78-87.

Joyce, S., & Nocera, J. (2021). *Global Digital Trust insights survey 2021. Cybersecurity comes of age.* PWC. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/assets/pwc-2021-global-digital-trust-insights.pdf

K-12 SIX. (2021). *The K-12 cyber incident map*. The K-12 Cybersecurity Resource Center. https://k12cybersecure.com/map/

Kelly, G. (2014, July 10). *Microsoft to abandon Windows 7 mainstream support. Pressure Builds On Windows 10*. Forbes. https://www.forbes.com/sites/gordonkelly/2014/07/10/microsoft-windows-7-mainstream-support/?sh=219786fc71f7

Kiesecker, C. (2020, September 7). *Top 10 back-to-school student privacy tips and resources for parents*. Parent Coalition for Student Privacy. https://studentprivacymatters.org/tag/selling-student-data/

Kronholz, J. (2014, April 1). *California's districts of choice*. Education Next. https://www.educationnext.org/californias-districts-choice/

Lake, J. (2018, December 18). *Encryption, hashing, salting – what's the difference?* Comparitech. https://www.comparitech.com/blog/information-security/encryption-hashing-salting/

Leal, F. (2009, February 17). *Students accused of changing grades using teacher's password.* The Orange County Register. https://www.ocregister.com/2009/02/17/students-accused-of-changing-grades-using-teachers-password/

Levin, D. A. (2021). *The State of K-12 cybersecurity 2020 year in review. https://k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf*, 2-6.

Liska, A. &. (2017). Ransomware. defending against digital extortion (1st edition). *O'Reilly.*

Liu, S. (2018, October). *Employee cyber security awareness training frequency in organizations in the United States as of 2018*. Statista. https://www.statista.com/statistics/949179/united-states-training-frequency-security-awareness/

Living security. (2020, January 27). *The disparity in the cost of security awareness training*. Living Security. https://www.livingsecurity.com/blog/how-much-security-awareness-training-cost

Livy, D. (2018, May 30). *What's the average IT service desk to employee ratio?.* Orange Matter. https://orangematter.solarwinds.com/2018/05/30/whats-the-average-service-desk-to-employee-ratio/

Mandaro, L. (2020, September 9). *Chromebooks gain share of education market despite shortages*. The Information. https://www.theinformation.com/articles/chromebooks-gain-share-of-education-market-despite-shortages

Martin Lee, W. M. (2017, May 12). *Player 3 has entered the game. Say Hello to 'WannaCry*. Talos Intelligence. https://blog.talosintelligence.com/2017/05/wannacry.html

Maylahn, P. (2015). CoSN 2015 K-12 IT leadership survey. *Association of American Publisher.*

McLoud, S. (2019, June 10). *I get paid for 180 days of work each year, but I actually work more than 250*. We Are Teachers. https://www.weareteachers.com/teacher-overtime/

Melendez, S. (2020, September 28). *Report. Hackers leak student data after Nevada school officials refuse to pay ransom*. Fast Company. https://www.fastcompany.com/90557175/report-hackers-leak-student-data-after-nevada-school-officials-refuse-to-pay-ransom

Michael Schwirtz (2021). Inside the ransomware industry. *New York, New York.*

Microsoft. (2008, March 24). *NTFS permissions for redirected folders (or home*

directories). Docs Microsoft. https://docs.microsoft.com/en-us/archive/blogs/migreene/ntfs-permissions-for-redirected-folders-or-home-directories

Microsoft. (2021). Microsoft authenticator. https://www.microsoft.com/en-us/account/authenticator

Microsoft. (2021, June 25). *Remote desktop clients*. Microsoft. https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-clients

Microsoft security advisory. Local administrator password solution (LAPS) now available. May 1, 2015. (2015, May 1). Microsoft Support. https://support.microsoft.com/en-us/topic/microsoft-security-advisory-local-administrator-password-solution-laps-now-available-may-1-2015-404369c3-ea1e-80ff-1e14-5caafb832f53

Morgan, S. (2021, March 13). *Global ransomware damage costs predicted to reach $20 Billion (USD) By 2021.* Cybercrime Magazine. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

Myers, L. (2021, June 4). *Ransomware attack response should extend beyond money to your team's morale*. Security Intelligence. https://securityintelligence.com/posts/ransomware-response-beyond-money-to-morale/

NASDAQ. (2021, May 14). *About 46 million Americans now own Bitcoin.* https://www.nasdaq.com/articles/about-46-million-americans-now-own-bitcoin-2021-05-14

National Cybersecurity and Communications Integration Center. (2016). *Malware trends.* Department of Homeland Security. https://us-cert.cisa.gov/sites/default/files/documents/NCCIC_ICS-CERT_AAL_Malware_Trends_Paper_S508C.pdf

Networking, C. f. (2018). *K12 cybersecurity cost report.* https://www.cosn.org/sites/default/files/cosn_cybersecurity%20cost%20report.pdf

Networks, Alvaka. (2021, March 20). *Ransomware recovery timeframes. how long does it take to recover?.* Alvaka Networks. https://www.alvaka.net/ransomware-prevention-recovery/#:~:text=Ransomware%20recovery%20timeframes%20can%20vary,given%20their%20%5B...%5D

NIST. (2017, June 7). *Digital identity guidelines.* NIST. https://pages.nist.gov/800-63-3/

NSA. (2019). Mitigating recent VPN vulnerabilities. *NSA.*

OCED. (2010*). The high cost of low educational performance the long-run economic impact of performing PISA outcomes. Program for International Student Assessment.*

O'Kane, P. (2018). Evolution of ransomware. *The Institution of Engineering and Technology Vol 7,* 321-327*.*

Oxeden, M. (2020, November 29). *Baltimore county schools say district-issued Chromebooks, Google accounts are ok to use after ransomware attack.* The Baltimore Sun.

Paganini, P. (2020, December 2*). K12 education giant paid the ransom to the Ryuk gang.* Security Affairs. https://securityaffairs.co/wordpress/111824/malware/k12-ryuk-ransomware.html

Panda Security. (2020, June 1). *Should I turn my computer off at night?*. Panda Security. https://www.pandasecurity.com/en/mediacenter/tips/turn-computer-off/

Pennell, C. (2020, May 04). *US schools struggle with EdTech challenge, as device types proliferate.* Futuresource Consulting. https://www.futuresource-consulting.com/insights/us-schools-struggle-with-edtech-challenge-as-device-types-proliferate/

Ponemon Institute. (2019). Costs and consequences of gaps in vulnerability response. *Service Now.*

Product notifications. (2020, March 16). https://www.sonicwall.com/: https://www.sonicwall.com/support/product-notification/sonicwall-s-

response-to-covid-19-coronavirus-and-the-increased-demand-for-a-remote-workforce/200317181233591/

Rajivan, P. A.-M. (2020). Update now or later? Effects of experience, cost, and risk preference on update decisions. *Journal of Cybersecurity. 1-12.*

Ransomware attacks on school districts. (2020). AM Trust financial. https://amtrustfinancial.com/blog/small-business/ransomware-attacks-on-school-districts

Rome, J. D. (2021). Understanding adoption barriers of superior technologies to authenticate and protect users from ongoing cyber threats. *ProQuest Dissertations Publishing.,* 75.

Schwartz, M. J. (2019, July 25). *Why hackers abuse Active Directory*. Bank Info Security. https://www.bankinfosecurity.com/hackers-abuse-active-directory-a-12825

Sciarretta, G. C. (2017). Anatomy of the Facebook solution for mobile single sign-on. Security assessment and improvements. *Computers & Security,* 71–86.

Seals, T. (2017, September 15). *Cost of user security training tops $290K per year*. Info Security Group. https://www.infosecurity-magazine.com/news/cost-of-user-security-training/

Security, C. f. (2020*).* Ransomware operators now auctioning stolen data. *Computer fraud & security*, 1-3.

Solutions, M. (2021). M-Trends 2021. Milpas. *FireEye, Inc*.

Studios, W. (2015). *Darkode [Recorded by K. P. Mills].* New York. https://www.wnycstudios.org/podcasts/radiolab/articles/darkode

Tarasawa, B. (2020, April 9). *COVID-19 school closures could have a devastating impact on student achievement.* NWEA. https://www.nwea.org/blog/2020/covid-19-school-closures-could-have-devastating-impact-student-achievement/

The return on investment (ROI) of security awareness training. (2019). Know Be4. Retrieved May 25, 2021.

https://www.knowbe4.com/resources/security-awareness-training-roi/

Top porn sites lead to malware. (2013, April 9). *Dynamoo's blog.* Dynamoo. https://blog.dynamoo.com/2013/04/top-porn-sites-lead-to-malware.html

Tsai, O. (2019, July 17). *Tech editorials*. Devcore. https://devco.re/blog/2019/07/17/attacking-ssl-vpn-part-1-PreAuth-RCE-on-Palo-Alto-GlobalProtect-with-Uber-as-case-study/

Verizon. (2021). *2021 data breach investigations report.* Verizon. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

Warner, R. (2017). *The detrimental effects of pornography on small children*. Net Nanny. https://www.netnanny.com/blog/the-detrimental-effects-of-pornography-on-small-children/

Weiss, E. G. (2019). *The teacher shortage is real, large and growing, and worse than we thought*. Economic Policy Institute. https://www.epi.org/publication/the-teacher-shortage-is-real-large-and-growing-and-worse-than-we-thought-the-first-report-in-the-perfect-storm-in-the-teacher-labor-market-series/

Weston, M. (2010). *Funding California Schools.* *https://www.ppic.org/content/pubs/report/R_310MWR.pdf*, 10.

Yan, Z. X. (2021). Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior.* 106791.

YubiKey 5 Nano. (2021). Yubico. Retrieved May 5 2021. https://www.yubico.com/product/yubikey-5-nano/