Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 1 Article 8

2023

# Examination of Cybersecurity Technologies, Practices, Challenges, and Wish List in K-12 School Districts

Florence Martin
*North Carolina State University*, fmartin3@ncsu.edu

Julie Bacak
*University of North Carolina Charlotte*, jabacak@uncc.edu

Erik Jon Byker
*University of North Carolina at Charlotte*, ebyker@uncc.edu

Weichao Wang
*University of North Carolina Charlotte*, WeichaoWang@uncc.edu

Jonathan Wagner
*University of North Carolina Charlotte*, jwagne31@uncc.edu

*See next page for additional authors*

# Examination of Cybersecurity Technologies, Practices, Challenges, and Wish List in K-12 School Districts


## Abstract

With the growth in digital teaching and learning, there has been a sharp rise in the number of cybersecurity attacks on K-12 school networks. This has demonstrated a need for security technologies and cybersecurity education. This study examined security technologies used, effective security practices, challenges, concerns, and wish list of technology leaders in K-12 settings. Data collected from 23 district websites and from interviews with 12 district technology leaders were analyzed. Top security practices included cloud-based technologies, segregated network/V-LAN, two-factor authentication, limiting access, and use of Clever or Class Link. Top challenges included keeping users informed, lack of buy-in from staff and decision-makers, lack of expertise to implement modern best practices, and cost of resources. Top concerns included possible cyberattacks, leaked student data, and lack of user awareness. Finally, their wish list included technology personnel, access to Clever of Class Link, external system diagnostic checks, professional development for staff, and replacing aging infrastructure. The findings have implications for K-12 administrators, technology leaders, and teachers.



## Keywords

Cybersecurity Technologies, K-12 School Districts, Technology Leaders

## Cover Page Footnote

This project was supported by the National Science Foundation - Award No 2122416



## Authors

Florence Martin, Julie Bacak, Erik Jon Byker, Weichao Wang, Jonathan Wagner, and Lynn Ahlgrim-Delzell

# Examination of Cybersecurity Technologies, Practices, Challenges, and Wish List in K-12 School Districts

Florence Martin
Teacher Educaiton & Learning Sciences
North Carolina State Univeristy
Raleigh, USA
fmartin3@ncsu.edu
https://orcid.org/0000-0002-6055-5636

Julie Bacak
Reading and Elementary Education
University of North Carolina Charlotte
Charlotte, USA
jabacak@uncc.edu
https://orcid.org/0000-0001-5436-4393

Erik Jon Byker
Reading and Elementary Education
University of North Carolina Charlotte
Charlotte, USA
ebyker@uncc.edu
https://orcid.org/0000-0002-2475-4195

Weichao Wang
Department of Software and Information Systems
University of North Carolina Charlotte
Charlotte, USA
WeichaoWang@uncc.edu
https://orcid.org/0000-0002-1969-0705

Jonathan Wagner
Department of Software and Information Systems
University of North Carolina Charlotte
Charlotte, USA
jwagne31@uncc.edu

Lynn Ahlgrim-Delzell
Educational Leadership
University of North Carolina Charlotte
Charlotte, USA
LynnAhlgrim-Delzell@uncc.edu
https://orcid.org/0000-0001-7881-650X

***Abstract*—With the growth in digital teaching and learning, there has been a sharp rise in the number of cybersecurity attacks on K-12 school networks. This has demonstrated a need for security technologies and cybersecurity education. This study examined security technologies used, effective security practices, challenges, concerns, and wish list of technology leaders in K-12 settings. Data collected from 23 district websites and from interviews with 12 district technology leaders were analyzed. Top security practices included cloud-based technologies, segregated network/V-LAN, two-factor authentication, limiting access, and use of Clever or Class Link. Top challenges included keeping users informed, lack of buy-in from staff and decision-makers, lack of expertise to implement modern best practices, and cost of resources. Top concerns included possible cyberattacks, leaked student data, and lack of user awareness. Finally, their wish list included technology personnel, access to Clever of Class Link, external system diagnostic checks, professional development for staff, and replacing aging infrastructure. The findings have implications for K-12 administrators, technology leaders, and teachers.**

***Keywords— cybersecurity, K-12 cybersecurity, technology directors, cybersecurity technologies***

## I. Introduction

As the need and demand for digital learning has grown, there has been a sharp rise in the number of cybersecurity attacks on K-12 school networks [1]. This has demonstrated a need for cybersecurity technologies and cybersecurity education which are lacking in most school districts across the US and around the world [2, 3]. Research includes some examples of cybersecurity education that some schools have adopted including cybersecurity simulations and summer-long workshops for teachers and students [4, 5]. However, there is still a gap in the literature related to cybersecurity education for school administrators and technology support staff [3, 6]. The irony of the lack of cybersecurity professional development for school administrators and school technology support staff is that both these groups are often the decision makers and represent the front line of planning and implementing their school's cybersecurity and data privacy plan. In this study, we examine K-12 technology leaders' perspectives on cybersecurity technologies used, effective cybersecurity practices, challenges, and wish list in addition to analyzing school district websites. This study was conducted as a needs assessment to develop professional development for K-12 technology leaders.

### *A. Cybersecurity Technologies and Practices used in K-12 Schools*

Cybersecurity technologies not only monitor student internet activity but also help identify and protect young children from related threats such as violence, self-harm, and suicide; child pornography, online predators, and sexual content; cyberbullying or other forms of online abuse; and drug or alcohol abuse. Researchers have broadly categorized internet risks as conduct, contact and commercial risks [7], and a number of cybersecurity technologies are used to prevent these risks. Some of the cybersecurity technologies include VPN software, multi-factor authentication service, monitoring software, antivirus software, internet filter etc [8, 9]. Research discusses the importance of connecting using virtual private networks to keep the users safe, especially when connecting from public wifis [10]. Monitoring software such as GoGuardian, DYKnow, Securely, LightSpeed, Gaggle are beginning to be used in K-12 schools [11, 12]. However, there is still a need for research to thoroughly examine the various cybersecurity technologies and practices used in K-12 schools.

### *B. Cybersecurity Challenges and Concerns in K-12 schools*

In K-12 schools, downloading malicious software and phishing are the most common cyber-attacks on a school's digital security and privacy [13, 14]. Research reported a plethora of cyberattacks in US public schools, which resulted in the disclosure of personal information, the loss of taxpayer dollars, and the loss of instructional time [15]. These cybersecurity vulnerabilities included phishing attacks, unauthorized disclosures, and security breaches or hacks that resulted in the disclosure of personal data [16, 17]. In June 2020, the Federal Bureau of Investigation [18] sent out a

security alert to K-12 schools about increased ransomware attacks on school systems as they transitioned to distance learning during the pandemic. Factors such as a large and dynamic user group having access to school networks and the unclear distinction between personal and professional use of computers contribute to vulnerabilities. Another cybersecurity vulnerability is the lack of software patching at US schools. For example, hundreds of US schools did not patch Microsoft Server Message Block two years after the patch was released, which resulted in increased vulnerability to ransomware and cyberattack [19]. Cybersecurity threats and vulnerabilities cannot be ignored by US school districts [2].

### C. *Needs Assessment Framework*

This study was conducted as a needs assessment for the design of professional development for administrators, technology leaders, and teachers. Understanding the technologies, effective practices, challenges, and wish list provides the essential information to develop this professional development to identify, protect, detect, respond and recover aligned with the Awareness-Ask-Action framework. We focused on the four aspects technologies, practices, challenges, and wish list to develop the professional development for technology leaders (Figure 1).

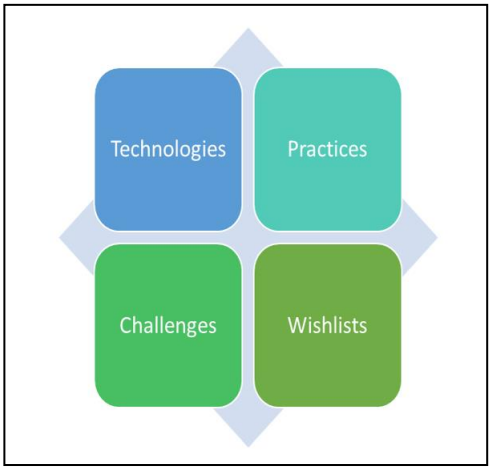


Fig. 1. Technologies, Practices, Challenges, and Wish list of Technology Leaders.

### D. *Purpose of the Study and Research Questions*

Professional development for technology leaders is important for addressing vulnerabilities to digital security in schools. In addition, understanding the cybersecurity technologies used, challenges, and wish list of technology leaders in schools are critical for effective digital teaching and learning to occur. In this study, we analyze school district websites and also examine K-12 technology leaders' perspectives on cybersecurity technologies used, effective cybersecurity practices, challenges, and wish list to address the following research questions.

1. What cybersecurity technologies are being used in K-12 school districts?

2. What are some effective cybersecurity practices and structures?

3. What are some challenges and concerns to cybersecurity and privacy in K-12 school districts?

4. What are some cybersecurity wish list from technology directors?

## II. METHODS

### A. *Research Design*

This study used a qualitative methodology and had two sources of data: 1) document analysis of 23 K-12 school district websites and 2) interviews with 12 technology directors. This qualitative study was conducted as a needs assessment to identify cybersecurity practices in K-12 school districts to support the technology leaders further through professional development. Both document analysis and interviews occurred concurrently at the beginning stages of this project.

### B. *Document Analysis*

A purposeful sample of 23 school districts from a Southeastern state in the United States were used in this study. The 100 school districts in this state were categorized into six groups based on student enrollment numbers: less than 2000 students, 2000 to 5000 students, 5000 to 10000 students, 11000 to 30000 students, 30000 to 75000 students, and above 75000 students. Twenty-three school districts were identified purposefully based on the district size to include representation for each of the six district types. The school districts' websites were examined for various technologies that were being used in school districts. This list of technologies was compiled in a document that was further categorized. In this article, we present the findings of cybersecurity technologies.

### C. *Interview Participants*

Interviews were conducted with 12 technology directors in a southeastern state in the US who volunteered to participate. Once institutional review board approval was received, the technology directors were recruited by identifying their email addresses from the school district websites and also by sharing the recruitment email with the leaders at the state level. These technology leaders had varied experiences in education and in their current roles. Table I includes information about these technology leaders. The interviewees commonly had the title of technology director but also had chief technology officer titles. In one instance, the technology leader served as a technology facilitator.

### D. *Data Collection*

Once consent was received from the leaders, the interviews were conducted virtually via Zoom. Each interview lasted approximately 30 minutes. Each interview participant received a $25 Amazon gift card as an incentive. The interviews were recorded using Zoom and transcribed using the Zoom machine-based transcription functionality, and then cleaned manually by a doctoral student researcher.

### E. *Data Analysis*

The transcribed data were coded by two members of the research team. The responses were compiled by questions and then two inductive coding cycles were used. The doctoral student coded all the interviews independently and the research methodology expert used the code book to independently code a random sample of 3 (25%) of the interviews to confirm the codes. They met to discuss any disagreements in the codes and 91% inter-coder reliability was obtained. Once all interviews were coded, the two researchers organized codes into axial codes [20] based on the common

patterns of response. Similar codes were further categorized using thematic analysis techniques [21]. These codes were shared with the rest of the team members to discuss the findings from the interviews.

TABLE I. TECHNOLOGY LEADERS PARTICIPANT DETAILS

| Technology Leader's Title | District/ Charter | Size of District/ Charter | Years in Education | Years in Current Role |
|---|---|---|---|---|
| Chief Information Officer | school district | Medium-large (over 12,000) | 28 | 8 |
| Information Technology Director | 9-12 charter school | Small (approx. 400 students) | < 1 | < 1 |
| Director of Technology | school district | Large (approx. 19,000) | > 30 | 5 |
| Technology Director | school district | Small (approx. 1600) | 16 | 6 |
| Chief Technology Officer | school district | Medium-large (about 16,000) | 22 | 7 |
| Chief Technology Officer | school district | Large (over 30,000) | 20 | 3 |
| Chief Technology Officer | school district | Small (less than 3,000) | 28 | 3 |
| Technology Facilitator | school district | Large (over 50,000) | 8 | 2 |
| Director of Technology | K-8 Charter school | (approx 400 students) | 8 | 4 |
| Director of Technology | school district | Medium-small(Approx. 7,000 students) | 40 | 1 |
| Technology Director | 6-12 charter school | small (approx. 700 students) | 13 | 5 |
| Director of Technology | school district | Medium-small (Approx. 6,000 students) | 17 | 2 |

## III. RESULTS

The following section provides findings from the website document analysis and interviews on 1) cybersecurity technologies used, 2) effective cybersecurity practices, 3) challenges/threats to cybersecurity 4) persistent concerns, and 5) cybersecurity wish list.

### *A. Cybersecurity Technologies Used in K-12 Schools*

From the website analysis and interviews, ten types of cybersecurity technologies were identified as being used in school districts: VPN software, Multi-Factor Authentication service, Monitoring software, Secure testing browser, Antivirus software, Internet filter, Challenge-Response software, Password Reset interface, Certificates, and End to end software environment support. Table II provides descriptions and examples for each type of these cybersecurity technologies.

TABLE II. CYBERSECURITY TECHNOLOGIES IN K-12 SCHOOL DISTRICTS

| Type of Cybersecurity Technology | Description | Examples |
|---|---|---|
| Virtual Private Network (VPN) software | Used to establish a secure network connection when accessing the internet using public networks | FortiClient VPN, "My CMS" intranet |
| Multi-Factor Authentication service | Approach where the user is required to verify their identity using two or more independent methods | Azure Active Directory |
| Monitoring software | Type of cybersecurity and surveillance software to monitor both user's online activities and operations on the computer | Gaggle, Downdetector, Bark for Schools, 8e6 Threat Analysis Reporter (for internet traffic), EducatorsHandbook.com Incidents+, DyKnow |
| Secure testing browser | Provides a secure online testing experience for students taking assessments | NWEA Secure Browser, SafeExamBrowser |
| Antivirus software | Protects one's computer against software viruses through monitoring incoming/outgoing traffic and user operations | Panda Antivirus, Microsoft Defender, Sophos, MalwareBytes, |
| Internet filter | Software that restricts what a user can access on the internet | Zscaler, Barracuda Spam Filter, |
| Challenge-Response software | An authentication method to prove the identity of the user | reCAPTCHA |

| | | |
|---|---|---|
| Password Reset interface | Provide a secure method for recovery/reset user password and prevent impersonation/DoS attacks | Tools4ever's SSRPM |
| Certificates | A verifiable digital evidence for the owner of online properties such as public keys or domain names | GoDaddy.com Web Server Certificate, Zscaler Root certificate |
| End to end software environment support | Provide software ecosystem configuration and maintenance support for smooth platform operation | Microsoft Premier Support, Managed Methods, |

### *B. Effective Cybersecurity Practices*

This section outlines practices that the 12 interview participants identify as the most effective cybersecurity practices in their districts. The top practices that were mentioned by the technology directors included cloud-based technologies (42%), segregated network/V-LAN (33%), two-factor authentication (25%), limiting access (25%), use of Clever or Class Link (25%) which is a single sign-on web and windows applications and access to files at school and in the cloud, phishing button in email (16%), PD/Sharing information (16%). One technology leader each mentioned the following practices, extra email security procedures for financial information (8%), remote desktop for Windows (8%), disabling inactive accounts (8%), limiting administration rights/nobody has the "key to the kingdom" (8%), external cybersecurity audit (8%) and password requirements (8%).

When discussing cloud-based technologies, one of the leaders mentioned "*we're trying to move as much of our technology to cloud-based services and pay to have someone manage it. Help us make sure it stays secure" and another participant stated "our school district is working to make all of our services cloud-based and try to drastically reduce the amount of physical equipment that we have, and also the storage of our data.*"

Also several of the leaders discussed two-factor authentication, and one leader specifically mentioned two-factor authentication on the cloud services "*But most of that is housed in the cloud and they still have to have that, every piece we've bought from them still has to have two-factor authentication before they can log in.*"

### *C. Challenges To Cybersecurity*

Participants described challenges related to maintaining cybersecurity. Their responses were focused primarily on two aspects of maintaining cybersecurity: end-users and resources. Challenges related to end-users included keeping staff and students informed (50%), not taken seriously by staff and decision-makers (42%), giving teachers autonomy while securing the network (25%), using devices/emails for personal use (25%), breaking longstanding bad habits (25%), pushback to change (25%) and lack of understanding of the long term consequences (8%). Challenges related to resources included lack of expertise to implement modern best practices (33%), cost of resources (33%), aging infrastructure (16%) and lack of manpower to investigate alerts (16%). A few other challenges were discussed which included ease of access (16%), managing large systems (8%), following federal guidelines (8%) and navigating terms of service/vendor communication (8%).

When discussing aging infrastructure as a resource challenge, for instance, one of the participants stated "*the biggest challenge is just the amount of legacy infrastructure. Our active directory environment started in 2006 and it's just been one patch after another, and one expansion of the schema for this program that we no longer use and that program that we no longer use. So just kind of that tech debt of legacy systems.*"

### *D. Persistent Concerns*

When the technology leaders were asked about "what keeps them up at night," participants described the following top concerns, worrying about cyberattacks such as ransomware, phishing, dormant attacks (33%), worrying about leaked student data (33%), lack of user awareness/understanding (25%), and resource availability in charter schools (16%). The following concerns were discussed by at least one technology leader including, tracking student usage/peak use time (8%), student email/passwords not changing (8%), inactive accounts (8%), lack of physical security compounding cybersecurity (8%), remote network access (8%), ease with which people can share data (8%), password security (8%), and staying up-to-date (8%)

One of the leaders who discussed the cyberattacks stated "*One of the biggest ones we had was that someone's firewall didn't get patched. It got exploited and then there was a cascade failure because they could get into the firewall. They got straight to the active directory server which then made it, they were able to put a payload where everybody who logs into the system now gets infected with everything it took. As everyone logged in for the day to check their email, everybody immediately got hit with a ransomware.*"

Another leader commented on the issue of cybersecurity attacks in charter schools because *"[often in charter schools], the person who's responsible for cybersecurity is also dealing with making the lunch order, and disciplinary issues and everything. And they don't have the access and the resources."*

### *E. Cybersecurity Wish list*

This section summarizes the resources the participants would include in their existing systems if money was not a factor. Resources included hardware, software, personnel, and training. In other cases, participants described actions they would like to implement but do not yet have the support to carry out. Specific names of products are shared when provided. When describing their "wish list" items, adding technology personnel was a common request, adding to the idea that no amount of new technology can really benefit the schools if the right people are not in place to support technology use. These resources included technology personnel (25%), access to Clever or Class Link (16%), external system diagnostic checks (16%), training for staff/paid training (16%), and replacing aging infrastructure (16%).

One technology director each discussed the following in their wish list, Microsoft Defender (8%), Azure Sentinel (8%), Cisco umbrella (8%), Fortinet (8%), Move to cloud (8%), Firmware (8%), New servers (8%), Training for tech staff

(8%), Biometric log-in (8%), Less access for students (8%), Encryption software (8%), Back-up and disaster recovery systems (8%), and Intrusion detection/prevention software (8%).

## IV. DISCUSSION

When examining the findings of this study collectively, the need for cybersecurity education and professional development in K-12 schools is apparent. While the most effective measures technology leaders referred to in interviews related primarily to infrastructure, the challenges they described were commonly connected to the actions, knowledge, information collection, and perceptions of the people within their districts, including both the staff who use the technology and the decision-makers who help secure needed resources. It is not surprising, then, that a common wish among the technology leaders interviewed includes more resources devoted to trained technology personnel, more equipment and software, and more professional development for their users.

### *A. Cybersecurity Technologies and Practices*

Though researchers have studied physical security in K-12 schools [22, 23], there is limited research on digital security in K-12 schools. Research discussed the importance of planning for cybersecurity in schools as they are an attractive target for data privacy crimes and that schools are repositories of large valuable data sets [6]. This emphasizes the rationale for implementing a number of cybersecurity technologies and practices in place. The cybersecurity technologies and practices identified in this study have implications for school district administrators as important technologies and practices that each school district should consider implementing. Table III outlines and summarizes the common cybersecurity technologies and practices in K-12 schools. What is noticeably missing from the practices column in Table III is ongoing professional development related to cybersecurity education for K-12 administrators, teachers, and technology support professionals in the schools.

TABLE III. SUMMARY OF CYBERSECURITY TECHNOLOGIES AND PRACTICES

| Cybersecurity technologies | Cybersecurity Practices |
|---|---|
| VPN software<br>Multi-Factor Authentication service, Monitoring software<br>Secure testing browser<br>Antivirus software<br>Internet filter<br>Challenge-Response software<br>Password Reset interface Certificates<br>End to end software environment support | Cloud-based technologies<br>Segregated network/V-LAN<br>Two-factor authentication<br>Limiting access<br>Use of Clever or Class Link which is a single applications<br>Phishing button in email<br>PD/Sharing information<br>Extra email security procedures for financial information<br>Remote desktop for Windows<br>Disabling inactive accounts<br>Limiting administration rights<br>External cybersecurity audit<br>Password requirements |

### *B. Cybersecurity Challenges and Concerns*

The technology leaders discussed several challenges and concerns which are summarized in Table IV. The challenges they discussed were primarily centered on these two areas: end-users and resources. A number of end-user challenges were due to lack of cybersecurity awareness or professional development on best practices related to implementing and sustaining cybersecurity practices. The second set of challenges were due to the lack of resources and expertise. The findings in this study showed the importance of dedicating resources for cybersecurity education, which would include professional development for the technology leaders and also for the technology facilitators and teachers. In addition, providing sufficient resources and personnel with the expertise is important. They also discussed a number of concerns and worries that kept them up at night which were due to some inefficient practices in place.

TABLE IV. SUMMARY OF CYBERSECURITY CHALLENGES AND CONCERNS

| Challenges related to End-Users | Challenges related to Resources | Cybersecurity Concerns |
|---|---|---|
| Keeping staff and students informed<br>Not taken seriously by staff and decision-makers<br>Giving teachers autonomy while securing the network<br>Using devices/emails for personal use<br>Breaking longstanding bad habits<br>Pushback to change<br>Lack of understanding of the long term consequences | Lack of expertise to implement modern best practices<br>Cost of resources<br>Aging infrastructure<br>Lack of manpower to investigate alerts<br>Ease of access<br>Managing large systems<br>Following federal guidelines<br>Navigating terms of service/vendor communication | Worrying about cyberattacks<br>Worrying about leaked student data<br>Lack of user awareness/understanding<br>Resource availability in charter schools<br>Tracking student usage/peak use time<br>Student email/ passwords not changing<br>Inactive accounts<br>Lack of physical security compounding cybersecurity remote network access<br>Ease with which people can share data<br>password security<br>staying up-to-date |

### *C. Cybersecurity Wish list*

Finally, the technology leaders discussed their wish list (Table V) which included several resources, and technologies. It is important for administrators to provide resources that support technology directors to keep their schools and school districts safe from cyberattacks [2, 19].

TABLE V. SUMMARY OF CYBERSECURITY WISH LIST

| Wish list for Resources | Wish list for Technologies |
|---|---|
| Technology personnel<br>Access to single-sign on services<br>External system diagnostic checks<br>Training for staff/paid training<br>Training for tech staff<br>Biometric log-in<br>Less access for students | Replacing aging infrastructure<br>Move to cloud<br>Firmware<br>New servers,<br>Encryption software<br>Back-up and disaster recovery systems<br>Intrusion detection/prevention software<br>Microsoft Defender<br>Azure Sentinel<br>Cisco umbrella<br>Fortinet |

### *D. Limitations*

This study was limited to school districts and technology leaders from one southeastern state in the United States. When selecting districts to include in the website analysis portion of this study, student enrollment size was considered in order to capture a range of districts. However, other considerations, such as the rurality of districts, was not considered when selecting districts. Additionally, while technology leaders from all districts in the state were invited to participate in this study, interviews were limited to volunteers who were available during the data collection timeframe.

### *E. Implications*

As educational technologies become more ubiquitous and necessary, it is critical that we protect the digital security and digital privacy of the vulnerable populations that depend on them. This highly-relevant work addresses a critical issue - cybersecurity in K-12 schools – by assisting us in understanding the networking and cybersecurity technologies used, the challenges, and the wish list of technology leaders in K-12 school districts. We found that one of the items on the wish list of technology leaders is the need for cybersecurity education. Indeed, the need for cybersecurity education could not be more timely. In the last five years, there have been increasingly greater cybersecurity threats to K-12 school districts across the United States [18]. For example, a ransomware attack on Los Angeles Public School in September of 2022 almost completely shut down the second largest public school district in the United States [24]. The ransomware attack required password changes for over 70,000 teachers and staff. More than 500,000 students' data were potentially compromised in this cybersecurity attack and about all of the students in Los Angeles Public School needed a password change because of the ransomware attack [24]. What shocked school district administrators the most was how quickly this ransomware took place over the Labor Day holiday weekend and how vulnerable the school district was to the cyberattack. Los Angeles was not the only school district to have encountered a massive cyberattack.

In this 2022 year, thus far, there have been cyberattacks in more than 25 school districts [25]. This includes a ransomware attack on Albuquerque Public Schools, which completely shut down the schools in this district for two days. Cyberattacks often equate to lost learning time for children and create quagmires for administrators, parents, school staff, and teachers. Cyberattacks on school districts became more prevalent throughout the COVID-19 pandemic as schools and teachers have had a great reliance on online technology. The need for cybersecurity education is an urgent implication of this study in light of the recent and growing cyberattacks on K-12 school districts. Cybersecurity education includes the development of knowledge and skills to protect hardware (i.e, laptops and digital devices), software, and digital systems, from unauthorized uses in order to ensure the confidentiality, integrity, and privacy of data [26]. The findings from this study also have an implication regarding the great need for cybersecurity education specifically tailored to school administrators, technology support staff, and teachers. Such cybersecurity professional development would support these school stakeholders in selecting and utilizing technologies that protect the privacy and security of student information. For example, cybersecurity education for teachers would include how to protect the technology being used for parental communication, to collect students' personal data, to collect assessment data, and to report out the grades. While many educational apps and tools have safeguards in place to protect student data and privacy, guidelines for cybersecurity protections are not universal, especially when teachers use applications with students that are less learning-focused. Researchers [26] assert that a school district's cybersecurity plans should be comprehensive and include consistent user training, data protection, firewalls, virus protection, and updates. Yet, as the participants in this study make clear: without cybersecurity education, the school administration and technology support staff may not be equipped or capable of implementing and sustaining the school's cybersecurity plan. The cybersecurity technologies used, and the effective cybersecurity practices help other schools and school district leaders get an understanding of the technologies used by their peers. The challenges and concerns of cybersecurity provide an opportunity for other researchers and practitioners to work on solutions to address the challenges. Finally, understanding the cybersecurity wish list provides an opportunity for administrators to provide the resources for the technology leaders to keep the schools and school districts safe.

### *F. Future Directions*

Additional research is needed on cybersecurity practices and professional development programs in school districts and schools. In this study, only 12 technology leaders and 23 school district websites in a southeastern state were used for data collection. A national representative study could be conducted to study cybersecurity technologies, practices, challenges and wish list across the country. Also, the studies can be conducted for different types of schools, and school districts. Survey-based research can be used to survey leaders from several schools and school districts.

## REFERENCES

[1] A. O. Opesade and A. O. Adetona, "An Assessment of Internet Use and Cyber-risk Prevalence among Students in Selected Nigerian Secondary Schools," *Journal of Cybersecurity Education, Research and Practice*, vol. 2, no. 3, 2020.

[2] D. Levin, "Unpatched school servers allow ransomware to flourish," The K-12 Cybersecurity Resource Center, https://k12cybersecure.com/blog/unpatched-school-servers-allows-ransomware-to-flourish/, May 2019.

[3] A. Rahman, N. A. Malaysia, M. T. U. K. Sairi, I. K. Zizi, and F. Khalid, "The Importance of Cybersecurity Education in School," *International Journal of Information and Education Technology*, vol. 10, no. 5, pp. 378-382, 2020, http://dx.doi.org/10.18178/ijiet.2020.10.5.1393.

[4] J. R. Hairston, , D. W. Smith, T. Williams, W. T. Sabados, and S. Forney, "Teaching cybersecurity to students with visual impairments

and blindness," *Journal of Science Education for Students with Disabilities*, vol. 23, no. 1, pp. 1-10, 2020, http://dx.doi.org/10.14448/jsesd.12.0007

[5] J. Ivy, R. Kelley, K. Cook, and K. Thomas, "Incorporating cyber principles into middle and high school curriculum," *International Journal of Computer Science Education in Schools*, vol. 4, no. 2, pp. 3-23, 2020, http://dx.doi.org/10.21585/ijcses.v4i2.101.

[6] M. Richardson, P. Lemoine, W. Stephens, and R. Waller, "Planning for cyber security in schools: the human factor," *Educational Planning Journal*, vol.2, no. 2, pp. 23-39,2020.

[7] M. Valcke, B. De Wever, H. Van Keer, and T. Schellens, "Long-term study of safe Internet use of young children," *Computers & Education,* vol. 57, no. 1, pp. 1292-1305, 2011.

[8] F. J. Harris, "CIPA/Internet filtering," *The International Encyclopedia of Media Literacy*, pp. 1-11, 2019.

[9] K. Haycock, "Blocking Access to Information and Ideas: The Use of Internet Filtering Software and Levels of Satisfaction in North American Schools," *IASL Annual Conference Proceedings*, pp. 121-132, 2021.

[10] R. Goldsborough, "Protecting yourself from ransomware," *Teacher Librarian,* vol. 43, no. 4, pp. 70, 2016.

[11] J. Bacak, F. Martin, L. Ahlgrim-Delzell, D. Polly, and W. Wang, "Elementary educator perceptions of student digital safety based on technology use in the classroom," *Computers in the Schools,* vol. 39, no. 2, pp. 186-202, 2022, https://doi.org/10.1080/07380569.2022.2071233.

[12] H. J. Krent, J. Etchingham, A. Kraus, and K. Pancewicz, "AI goes to school: implications for school district liability," *Buffalo Law Review,* vol. 67, no. 5, pp. 1329-1344, 2019, http://dx.doi.org/10.2139/ssrn.3656698.

[13] R. Prasad and V. Rohokale, *Cyber security: The lifeline of information and communication technology*. Switzerland: Springer, 2020, http://dx.doi.org/10.1007/978-3-030-31703-4.

[14] S. P. Prem and B. I. Reddy, "Phishing and anti-phishing techniques," *International Research Journal of Engineering and Technology,* vol. 6, no. 7, pp. 1446-1452, 2019.

[15] R. Chang, "Educational technology strategies publishes K–12 cyber incident map," 2017, https://thejournal.com/articles/2017/03/31/ed-tech-strategies-publishes-k12-cyber-incident-map.aspx.

[16] The Hacker News, "Using Breached Password Detection Services to Prevent Cyberattack," 2022, https://thehackernews.com/2022/10/details-released-for-recently-patched.html.

[17] R. Lakshmanan, "Details Released for Recently Patched new macOS Archive Utility Vulnerability," 2022, https://thehackernews.com/2022/10/details-released-for-recently-patched.html.

[18] Federal Bureau of Investigation, "Private industry notification, 20200623-001, ransomware targeting of K-12 schools likely to increase during COVID-19 pandemic," 2020, Washington, DC: FBI.

[19] S. Gallagher, "Wanna cry? Hundreds of US schools still haven't patched servers. ArsTechnica," May 2019, https://arstechnica.com/information-technology/2019/05/two-year-after-wannacry-us-schools.

[20] A. L. Strauss and J. M. Corbin, *Basics of qualitative research: Grounded theory procedures and techniques.* Sage, 1990.

[21] J. Saldaña, *The coding manual for qualitative researchers.* Thousand Oaks, CA: Sage, 2021.

[22] F. J. Davies and G. Bernardo, "An overview of physical security technology for schools: What security technologies to consider for schools—finding a direction," *The Handbook for school safety and security*, pp. 133-144, 2014.

[23] E. Taylor, *Surveillance schools: Security, discipline and control in contemporary education*. Springer, 2013.

[24] H. Blume and A. Reyes-Velarde, "Student information remains at risk after massive cyberattack on Los Angeles Unified," *Los Angeles Times*, Sep. 5th, 2022.

[25] National Public Radio, "A cyberattack hits the Los Angeles School District, raising alarm across the country," *National Public Radio*, Sep. 7th, 2022, https://www.npr.org/2022/09/07/1121422336/a-cyberattack-hits-the-los-angeles-school-district-raising-alarm-across-the-coun.

[26] A. Sobel, A. Parrish, and R. K. Raj, "Curricular foundations for cybersecurity," *Computer*, vol. 52, no. 3, pp. 14-17, 2019, http://dx.doi.org/10.1109/MC.2019.2898240.