# Making the Case for Increased Investment in Cybersecurity

## A Primer for K12 School Districts just getting started with Cybersecurity

**CoSN RESEARCH REPORT**
September 2022

Prepared by:
Omar Chaudhry,
Charles Blaschke
Scholarship Fellow

CoSN
LEADING EDUCATION INNOVATION

### About CoSN

CoSN (Consortium for School Networking) is the premier professional association for K-12 school system technology leaders. CoSN provides thought leadership resources, community best practices and advocacy tools to help leaders succeed in the digital transformation. Today, CoSN represents over 13 million students in U.S. school systems/districts and continues to grow as a powerful and influential voice in K-12 education.

### Blaschke Fellowship Fund

The Blaschke Fund was created in 2019 to support emerging leaders in education technology policy and advocacy. The memorial fund honors the late Charles Blaschke, who conducted pioneering research and analysis on the ever-changing U.S. education landscape for over 50 years. The Blaschke fellowship is designed to give graduate students in public policy and/or education an opportunity to work with CoSN on education policy projects. Priority is given to initiatives focused on national education technology issues, such as funding, legislation and/or policies. Policies could include ensuring digital equity, protecting privacy of education data, enabling accessibility or other key topics.

### Omar Chaudhry

Omar Chaudhry is the 2022 Blaschke Fellow and he compiled this report. Omar has a B.A. in Management from Marymount University and an M.S. in Cybersecurity from Old Dominion University. He is currently serving as an Information Technology Support Specialist for the National Association of Counties in Washington, DC.

## Executive Summary

IT infrastructure often competes for attention with many priorities within K-12 school systems. Cybersecurity mitigation often lacks the funding needed to provide a strong defense against rising threats in the current environment. It would be natural to come to the conclusion that maintaining a critical set of cybersecurity controls in school systems is a highly costly endeavor in both time and money. As most collaborative learning and workspaces migrate to virtual or hybrid environments with the emphasis of using newer technology, it's hard to overlook the challenges that come with upgrading a school's network infrastructure. As cyber attacks aimed towards school systems are becoming regular occurrences and more sophisticated, everyone from students, staff and faculty will have become more cyber security savvy. These attacks vary in their implementation, including ransomware, data theft, phishing and cyber vandalism. This report addresses these risks towards K-12 schools as well as effective strategies to protect against them, especially for those just getting started.

This report identifies five actions a school system IT staff might take now or in the near future to better defend IT infrastructure:

1. Train IT Staff and End Users
2. Add Technical Expertise to your IT Team
3. Secure the network
4. Create a sustainable plan to replace equipment at regular intervals
5. Create an environment of certainty for the IT Function with leadership buy-in and reliable funding

## Why It Matters

With so many nefarious threats currently facing our schools and students — from school shootings to cyberbullying — it's more important than ever to protect students and teachers from cyberattacks. Cyberthreats are dramatically increasing and will only continue to grow in sophistication and prevalence. Schools need to be more proactive in taking steps to prevent not just compromised school hardware, but stealing the identities and confidential information of minors and educators. The harsh reality is that today's school districts must deal with increasingly sophisticated cybercriminals who are targeting schools with malware and ransomware to extort money from them. Large data breaches using insecure passwords leave students and staff vulnerable to identity theft. Cyberattacks on student records can have serious consequences for minors and their families. Just looking at the threat of global ransomware, 64 percent of organizations in higher education and 56 percent in K-12 suffered ransomware attacks in 2021.[1]

School systems are facing this increasing  burden of defending their networks with minimal dedicated staff resources. CoSN's 2022 K-12 EdTech Leadership Survey[1] identified cybersecurity as the number one priority for school system technology administrators. Yet this survey also showed that only "a fifth (21 percent) of districts have a full-time equivalent (FTE) employee dedicated to network security, the same percentage as the prior year." Under staffed school district technology teams are dealing with the growing magnitude of the cybersecurity threats. "The global education sector was hit by more than twice the industry average of cyberattacks last month, according to a new report by Check Point Research. The cyber intelligence provider claims that education and research has suffered a 114 percent increase in the past two years, making it comfortably the most attacked industry sector."[2] According to the (Multi-State ISAC) Center for Internet Security, K-12 has been the most impacted public sector for Ransomware (57percent in fall 2020), largely because schools were a "soft target" for cybercriminals before COVID.

While some solutions do exist to protect data from cybercriminals, they can be  costly. Another issue facing schools today is that many IT departments are strapped for funding, especially for maintaining software patches and antivirus updates, protecting school data from cyberattacks and educating staff and students about cyber threats. Remote learning and work environments in schools require IT teams to be more diligent than ever to

[1] How Does K-12, Higher Education Fare In A Ransomware Attack?, Governing Magazine, April 2022.
[2] Education sector most at risk of cyber attack, Checkpoint research, August, 2022.

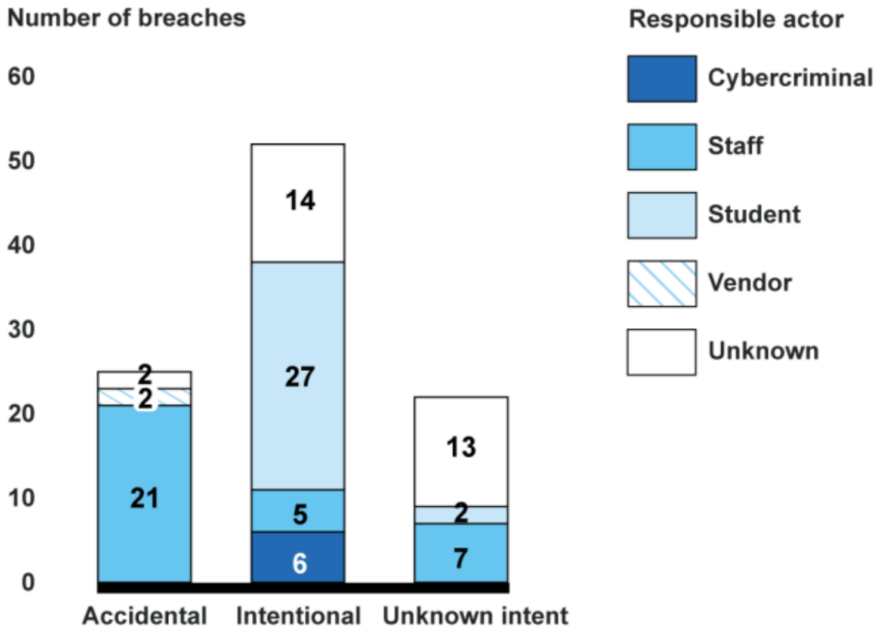
ensure they have control over what devices and applications students can access. This can mean having to install more endpoint security solutions that connect to servers remotely and encrypt data to ensure student and educator personal information remains secure.

## Examples of Risks to K-12

Cyberattacks on K-12 school systems are increasingly the norm, and they are an inevitable threat that students, staff and faculty will have to look out for. Attacks may vary in their implementation, sometimes through ransomware and data theft, to phishing and cyber vandalism. This report addresses some of the more common risks towards K-12 schools as well as effective strategies to protect against them.

According to General Accounting Office's (GAO) analysis of K-12 Cybersecurity Resource Center (CRC) data from July 2016 to May 2020, thousands of K-12 students were affected by 99 reported data breaches, a type of cybersecurity incident in which data is compromised. Students' academic records, including assessment scores and special education records, were the most commonly compromised type of information (58 breaches). Records containing a student's personally identifiable information (PII), such as Social Security numbers, were the second most commonly compromised type of information (36 breaches).

**Responsible Actor and Intent of Reported K-12 Student Data Breaches**
**July 1, 2016 – May 5, 2020**




*Source: GAO analysis of K-12 Cybersecurity Resource Center data | GAO-20-644*

Statistics may significantly undercount the true extent of the problem as many breeches are not reported.

# Recommended Actions

School Districts must defend against various cybersecurity threats, yet do so within the constraints of their current staffing and technical resources. These threats, best practices and resources to help a school system combat them are listed  in priority order.

## 1. Train IT Staff and End Users

Training is the best defense against cybersecurity threats that seek to leverage end users as a point of entry into school systems. IT staff should be trained to identify and mitigate threats. End users should be trained to identify and avoid threats and report these threats to the IT department. Asynchronous training offers the greatest flexibility given conflicting schedules, and there are excellent asynchronous off the shelf programs available to support school districts. Almost all of the School Districts participating in the CoSN Peer Review program, a program that brings in outside experts onsite to review practices in that district, deploy an asynchronous training system to train end users. Some districts offer a program of remedial training for those users that continue to open planted phishing messages after receiving training.

Best Practice: Incident Response Planning. Districts should have a robust incident response plan in place. An incident response plan is a set of procedures that an organization follows when responding to a security incident. One way to develop and practice your plan is to have your team participate in a tabletop role playing game where you act out various cybersecurity incidents and staff roles and responsibilities. Any team looking for ideas for incident response tabletop exercises can look at CoSN's online Cybersecurity Leadership Game. The game contains many incident response scenarios that can be used in planning a tabletop event.

## 2. Add Technical Expertise

Staffing experienced and certified IT staff in K-12 school districts is probably the most challenging investment a school district can make if they are struggling with locating and funding the cost of cybersecurity expertise. It is important to note that hiring skilled IT staff does not require hiring only seasoned professionals with years and years of experience. One could argue that many cybersecurity roles do not require a four-year undergraduate or graduate degree. School systems may want to consider cybersecurity candidates who have a two-year associate's degree or are in community college pursuing

their degree or have cybersecurity certificates as an alternative. Also, in some communities, districts either use an education service agency or state service for monitoring cybersecurity. And, some companies are now providing part-time CISO remote support.

According to the most recent EdTech Leadership Survey Report conducted by CoSN[3], the majority of respondents said their districts were understaffed in two IT functions that have direct impact on teaching and learning: providing instructional support around classroom use (52 percent) and providing remote support to students and families (51 percent). The shortage can result in potentially inexperienced IT staff taking on added levels of responsibility that require the skills and experience of a more qualified IT professional.

**Staffing Levels by IT Function**

| IT Function | Understaffed | Adequate | Overstaffed |
|---|---|---|---|
| Provide instructional support around classroom use | 52% | 47% | 1% |
| Provide remote support to students and families | 51% | 49% | 0% |
| Integrate technology into the classroom | 46% | 53% | 1% |
| Support device cleansing protocols | 42% | 58% | 0% |
| Plan and implement new technology | 41% | 58% | 0% |
| Effectively support the needs of the district/school | 39% | 61% | 1% |
| Provide remote support to teachers and other educators/administrators | 35% | 65% | 1% |
| Meet your department's yearly objectives | 26% | 74% | 1% |
| Maintain network systems adequately | 25% | 74% | 1% |
| Maintain applications | 22% | 78% | 1% |
| Install applications | 15% | 84% | 1% |

*Source: 2022 CoSN Ed Tech Leadership Survey*

For those districts that are able to staff full time cybersecurity professionals, a collaboration between CoSN and SETDA (2022) found that the job descriptions for cybersecurity professionals fall into the following areas of focus:

- Leadership and management including policy and compliance

[3] 2022 CoSN Ed Tech Leadership Survey https://www.cosn.org/edtech-topics/state-of-edtech-leadership/

- Network and systems defense/ Security analysis
- Security operations and incident response
- Training, education and awareness

Even if there is funding for such positions it likely is hard to compete with the private sector and recruit cybersecurity staff.

Unfortunately, the vast majority of districts do not have funding for a full time cyber security specialist. If that is the case at your district, consider budgeting for it next year while adding cybersecurity responsibilities to your current IT staff descriptions now. Most K-12 technology positions fall into one of these categories:

- Chief Information Officer (CIO), Chief Technology Officer (CTO) or IT Director
- Network or Systems Analyst
- Applications Developer
- Service Desk, Help Desk, or end user support

Each of these position descriptions should include specific cybersecurity expectations and clear delineation of cybersecurity responsibilities. This will ensure that K-12 technology staff are aware of the cybersecurity requirements of their positions and be able to execute on those requirements. In addition to including cybersecurity in the position descriptions, initial and ongoing training is necessary to ensure that staff are able to follow through with their responsibilities.

Best practice: Add a standard statement of expectation around cybersecurity to each position description. The following is an example of a standard statement your district could use:

> Proactively securing and protecting <district's> digital assets and information systems and supporting cyber safety is crucial to our mission of teaching, learning and preparing students to be college and career ready. All <name> district's IT professionals are directly responsible for providing high-quality and secure IT systems and services. Persons in technology roles are expected to be responsive to security-related actions and requirements, and to collaboratively find secure ways to support the <insert name> district.

Resources: Cyber Safety: Seven Security Steps
Cyber Safety Social Media Messaging Campaign

**Case Study**

The number of unfilled cybersecurity jobs worldwide grew 350 percent between 2013 and 2021[4]. There is a clear shortage of IT and cybersecurity professionals in the workforce. One school district is taking on the challenge of teaching their own students how to fight cyber crime.

The *Cyber Academy* is an innovative program implemented by Lakota County Schools (OH). It is a program designed alongside industry partners to develop a local pool of talent in the lucrative field of cybersecurity. It provides students the resources and training necessary to fight cyber crime. With a wide range of industry-recognized cyber-focused courses, the curriculum is filled with highly valued certification opportunities and includes labs and a digital library.

The program is made up of three courses that are designed to partner hands-on, in-class challenges with online preparation for industry certifications in cyber security.

> Cyber 1: Starts with in-class challenges that are tackled with support from industry partners. Each student in the Academy is matched with a mentor in the field to serve as a resource and help guide students through the program and beyond.
> Cyber 2: Students experience job shadowing with industry partners to see the world of cyber security in action. They also work with their mentors to solve in-class challenges.
> Cyber 3: Culminates in a "build your own challenge" experience, through which students can define the path and certifications that most interest them. The program ends with a paid internship in either the spring or summer of the student's senior year.

This is a great idea for districts struggling to fill IT positions and an incredible opportunity for students in your district to learn in demand skills.

## 3. Secure the Network

Securing the network is one of the most important actions a school system can do to thwart cybersecurity threats. With threats constantly evolving, IT teams need to know all

[4] Sydney Lake. June 30, 2022. Companies are Desparate for Cybersecurity Workers - More than 700K positions need to be filled.
https://fortune.com/education/business/articles/2022/06/30/companies-are-desperate-for-cybersecurity-workers-more-than-700k-positions-need-to-be-filled/

potential threats and vulnerabilities. In this section we will explain the different types of attacks and how you can best defend against them.

Best Practice: Hire an outside “trusted partner” firm to perform a penetration test for your district. This will expose the weaknesses in your systems and infrastructure. It is ideal to have an external vendor perform this test every 18 months. Having a list of weaknesses will help you make the case to the leadership team for more investment and resources to support cybersecurity.

Be familiar and adopt a cybersecurity framework such as the one provided by the National Institute of Standards and Technology (NIST) or CIS Controls. Adopting a known framework provides a tool to support conversation and decision making. These frameworks can seem complex and overwhelming to the new practitioner. The best approach is to recognize that no organization can implement all recommendations at once, and to create a plan for incremental implementation. The CIS Controls make this easy by prioritizing the order in which to do the work through the CIS Controls Implementation Groups.
Resources: NIST Framework
CIS Controls

## Cybersecurity Threats

### Social Engineering

Social engineering is a manipulation tactic used by hackers or cyber criminals to gain unauthorized access to personal information or systems. Criminals use a variety of social engineering tactics to try and trick people into giving their personal information or allowing access to an organization's systems. For example, a hacker could send emails pretending to be a bank or other suppliers to try to get people to click on a link that will send them to a fraudulent site that looks exactly like the real thing. These phishing emails often contain attachments or links that will install malware in the system or steal personal information such as usernames, passwords and credit card details.

These phishing attempts often involve hook stories and fear tactics to try and manipulate people to respond. Criminals use phishing emails to trick employees to provide access to the district network, then allowing them to capture personal information. There are countless examples of phishing emails targeting schools that try to steal sensitive

information from students and staff. Students and staff are particularly vulnerable without training.

**Ransomware**

Ransomware infects computers and encrypts files so that the files cannot be accessed or used by users. Once the ransomware has successfully infected a device, the user is alerted that their data has been encrypted and that the only way to restore their data is to pay a fee. If a victim refuses to pay, his or her data can be permanently lost. Even if the victim pays the ransom, there is no guarantee that his or her data will be decrypted and access regained by the school district.

According to Symantec[5], paying the ransom does not guarantee that victims regain access to their decrypted data. The attackers threaten to permanently delete the data unless the victim pays the ransom before a deadline set by the attackers. However, once the ransom is paid the criminals often fail to remove the encryption and the victim is left with useless data. The ransomware threat is serious and is growing every day.

In addition, the cyber criminals often do not stop with just one attack. They continue to send more sophisticated ransomware and are targeting new industries every day. The best way for schools to protect themselves is to train their staff and students to be cautious and report suspicious emails or websites immediately to IT personnel.

Best Practices: Develop a confidential Ransomware Plan and practice it.

Resources: Preventing a ransomware attack is possible. However, it takes careful planning, training, and attention to cybersecurity fundamentals. Ransomware Brief

**Data theft and privacy**

Data theft and privacy is a concern when it comes to cyber attacks on schools. If confidential student information is leaked, this can have serious consequences for the minors and their families. While various solutions exist to protect data from cybercriminals, many are cost prohibitive for K-12 districts. Protecting data is an essential responsibility of districts whether the data is stored locally, hosted in the cloud, or with a third-party provider.

---

[5] Ransomware Payments are Fueling the Ransomware Scourge. Adam Bromwich. June 14 2021. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/targeted-ransomware-ecosystem

Best Practices: Backup data both in the cloud and on premises. Part of planning for cybersecurity is being realistic about its occurrence. Loss of data by way of crashes or breaches can wreak havoc on internal systems. Data backups are key to your District's disaster recovery strategy. Data backups ensure that you can recover district data if it is lost or stolen within an affordable time frame. Your district should have multiple places to backup data both in the cloud and on premises; additionally it should be scheduled and tested frequently.

Read privacy policies of third party applications and cloud providers carefully. Any new software or application needs to be vetted thoroughly before staff and student use. It is a best practice to create a system for approving new software that reaches high levels of leadership.

Resources: Protecting Privacy in Connected Learning Toolkit (CoSN)

Privacy and Online Tracker (CoSN)

Cloud Technology is becoming more popular in schools: here's what a school system can do to stay secure Part 1 & Part 2

Cloud Computing (scroll down for cloud resources)

**Student Hacking**

One of the biggest risks that schools face is the threat of student hackers. Student hackers are an internal threat to schools that carry out attacks that can be intentional or not. Sometimes students will find unsecured data just by being curious. Other times teachers or administrators leave passwords on their desks and other unsecured locations. While student hackers are not typically considered to be a serious threat, they can pose a significant risk to schools if they gain access to sensitive data or systems.

Another aspect to be wary of is students launching attacks using scripts. They often lack the technical skills to create their own tools and instead rely on others to do the work for them. They can cause significant damage is why districts should take steps to protect their networks from these types of attacks. They are a threat because they can easily exploit vulnerabilities in systems that are not properly secured. This can lead to data loss or theft, and in some cases, denial of service attacks.

Best Practices: The school system has effective architecture, design, and maintenance to support current and emerging security concerns, including virus/malware protection, intrusion detection, patch management, and application controls.

Resources: Cyber Security Toolkit - Authentication Management

**Classroom Management to Prevent Insider Threats**

As discussed earlier, insider threats pose a significant risk that can be initiated by staff as well as students. According to Batavia county public schools, one of the most important factors to consider is proper classroom management. Tony Inglese, Chief Financial Officer of Batavia Public School District 101, believes that technology leaders need to, "make sure that teachers really know how to use these video conferencing settings to filter what they want to permit and what they don't want to permit. Batavia schools discovered, during the pandemic, that a lot of technology they were using to conduct online classes was not built with classroom management in mind."

Classroom management is  vitally important when it comes to preventing students from engaging in malicious activities while at school. This can be difficult because many students are not easily controlled. If teachers and administrators do not have strong classroom management skills, students may be more likely to engage in cyberattacks or other malicious behavior that could compromise the school's network.

Classroom management, in this context, refers to familiarizing teachers with video conferencing features when teaching virtually. This will prevent disruptive behavior in the virtual learning environment, which could potentially incite an insider threat such as student hacking. However, it's important to also consider the fact that classroom management requires a positive relationship between teachers and students, which will lessen the likelihood of disruptive behavior in the virtual classroom.

Best Practices: The school system maintains processes and systems to protect student and staff personal information.
Appendix 3

**Vulnerabilities in Hybrid and Remote Learning**

With additional hybrid and remote learning there is more cyber risk. Students and staff using their devices at home on less secure networks, can unknowingly bring malware back into the school network from their home and other public networks (libraries, coffee shops, etc.). Also when students/staff use their personal devices to access cloud or web-based applications, there is a risk of unauthorized access since the security measures to use those devices are not standardized.

As districts have implemented more hybrid and remote learning, the reliance on cloud technology has increased. Unsecured remote access to a district's data whether in the cloud or at a district's data center, opens the door to compromise of the data. The primary risks to computing include: data privacy compliance, data breaches, unauthorized access, malware infections and cyber attacks[6]. Since cloud computing is not going away, your district should take steps to secure your cloud network, systems and data.

Best Practices: Implement multi factor authentication (MFA) when using the VPN to remotely access school systems. According to Microsoft, strong authentication can protect against 99.9 percent of identity attacks[7]. Restrict control of access to third party applications. Restrict administrative access to only those users that need this access to effectively manage the system.

Resources: Video Conferencing Tools in the Age of Remote Learning: Privacy Considerations for New Technologies

## 4. Create a sustainable plan to replace equipment at regular intervals

Computer hardware manufacturers are slowly shifting to customized silicon for their equipment, and trends in computer design have made their devices less and less repairable.

---

[6] Cybersecurity and Cloud Computing: Risks and Benefits. 1/18/2022. Zainab Al Mehdar. https://rewind.com/blog/cybersecurity-and-cloud-computing-risks-and-benefits/

[7] New Insights on Cybersecurity in the Age of Hybrid Work. October 27, 2021. Bret Arsenault. https://www.microsoft.com/security/blog/2021/10/27/new-insights-on-cybersecurity-in-the-age-of-hybrid-work/

**Hardware & Device End of Life**

A key cybersecurity defense is getting new devices when a manufacturer announces end-of-life (EOL) status to their older devices.

- When manufacturers announce end-of-life for a device, it means that the device is no longer being manufactured and will no longer be supported by the manufacturer. This can be a problem for schools, as they may not be able to get new devices when they need them. One way to mitigate this problem is to get devices from a manufacturer that offers extended support for end-of-life devices.

- If not addressed upon a manufacturer's announcement, EOL hardware can present long term risks to school districts in terms of cybersecurity[4]. This is because outdated software vulnerabilities are no longer patched by the device's manufacturing company, leaving the door open for malicious actors to exploit them. In addition, end-of-life equipment is often unsupported by the manufacturer in both hardware and software, meaning that school districts will have to find other ways to keep their systems secure. Once hardware and software reach the end of their life cycles, they are no longer supported by manufacturers. This means that if something goes wrong with the product, there is no one to turn to for help.

Best Practices: There are a number of additional security practices that schools can implement to help protect their students and staff from cyberattacks. These practices include things like using strong passwords, and encrypting data. Schools should also educate their students and staff about cyber threats and how to protect themselves. Closing network ports, installing updates and additional supervisory checks for abnormal network behavior are all practices that might not need extensive training and can just be added to regular duties and responsibilities.

The best practice in protecting a school's computer systems is to limit the amount of administrative privileges that users have on their machines. This can reduce the chances that a user will be able to infect the computer system with malware or otherwise compromise the security of the system. However, it should be noted that this can pose a challenge in schools where teachers and other staff members need to access certain files that are stored in restricted locations on the computer system. In this case, it may be best to allow limited administrator privileges but monitor their use carefully to ensure that

users do not attempt to abuse these privileges by attempting to install software, for example, in restricted areas.

Resources: Are Your Systems Ready for Fall Term 2022 (CoSN Blog)
Technology Sustainability Toolkit (Verizon/Digital Promise)

## 5. Create an environment of certainty for the IT Function with leadership buy-in and reliable funding

**Leadership buy-in**

Districts should strive to create certainty around the management and funding for IT. The Districts most successful with this have both a shared vision for technology and a collaborative executive management team. According to the CoSN IT Leadership Report Survey 2021, 57 percent of IT leaders reported directly to the superintendent. Being part of the Superintendent's cabinet enables IT Leaders to participate in planning how technology can be leveraged to support district goals. At a minimum, districts need to have a system in place to include their IT Leaders as part of cabinet-level conversations around priorities and expenditures. It is with collective decision-making that a comprehensive funding model can be created to directly support the technology plan.

Best Practice: School system leaders have created a shared vision for creating and sustaining a digital environment that is aligned with the school system strategic plan and goals. A cross-functional executive leadership team meets periodically to monitor and communicate progress. The CTO is included in these discussions.

**Resources:** Protecting Privacy: Making the Case to Leadership
Security Planning Template
Self-Assessment (District Security Checklist)
The Importance of Cybersecurity

**Financial Limitations**

Regardless of a school's budget, there will always be financial constraints. However, underfunded school districts will experience harsher restrictions and dire consequences without a dedicated budget to invest into newer equipment. Without proper funding towards IT protection, schools will open themselves to cyberattacks. This is a

non-negotiable issue, as an IT team will at some point or another require to invest some level of funding in order to upgrade their technology, be it in hardware or software.

However, there are a few ways that public schools can mitigate the costs of upgrading hardware. One is to sell the old devices through school equipment resellers. This can help to offset the cost of purchasing new devices. Another option is to transfer the software keys of usable software from the old devices to the new ones. This way, schools can still use the software even though the hardware is no longer supported.

A second strategy is to consider installing open-source software and operating systems such as Linux. Open-source software and operating systems are free, community-run and are not associated with any one company. This means that they will continue to be updated and supported even after a device is no longer supported by the manufacturer. This can help to extend the life of hardware and save money for public schools. However, this strategy requires higher internal technical expertise and may not be realistic for many school systems, especially those with small technology teams.

Best Practice: The school system has funding plans and approaches that assure the long-term sustainability of school system technology resources.

Resources: Working together for Student Success. CoSN & ASBO.

## Conclusion

Act now! The best way for you to protect your district and its students from cyber threats is to be proactive. Here are actions you can take today that will better prepare your district for an attack.

**Training.** Train staff and students on what social engineering attacks look like. Repeat training each year and update as new types of threats emerge.

**Limit administrator privileges and access to Personal Identifiable Information (PII).** Access to PII and financial information should be guarded on a must have basis. Restrict administrative access to only those users that need this access to effectively manage the system.

**Update software on existing equipment.** Delaying updates leaves your network vulnerable to attacks. Ensure users are not bypassing updates.

**Audit your Network.** If you can't afford to hire an outside third party at the moment to conduct an assessment of your network, start with your team. Look for weaknesses and come up with a plan of action to address them.

**Advocacy.** Check CoSN's policy updates for opportunities to advocate for better policies at the state and federal level. Make the case for additional investment to the leadership in your district.

For additional resources on cybersecurity see CoSN's resource library and upcoming events.

# Appendix 1

## Hack Me If You Can: Teaming Up with Student Hackers

One of the most overlooked insider threats to a school is a student hacker. It can be tough to determine if student hackers are just script kiddies looking to cause mischief, or if the hacker is just interested in learning through hacking. Script kiddies are amateur hackers who typically use pre-existing tools and scripts to launch attacks. They often lack the technical skills to create their own tools and instead rely on others to do the work for them. While script kiddies are not typically considered to be a serious risk, they can pose significant problems to schools if they gain access to sensitive data or systems. According to the 2022 CoSN Ed Tech Leadership Report, district technology leaders believe that 42 percent of insider threats were more of a risk to schools compared to outside hackers and ransomware attacks.

Student hackers can be dangerous as they can easily launch attacks that can cause significant harm to a school system, other students and educators. This can transition from accidental damage to genuine malicious intent if not addressed in an appropriate fashion. Script kiddies do still count as a potential risk to schools if they are not addressed. Without any intervention, they evolve into a threat because they can easily exploit vulnerabilities in systems that are not properly secured. This can lead to data loss or theft, and in some cases, denial of service attacks.

While it can be natural to conclude that schools should just implement a stricter security framework in order to detect and mitigate threats like script kiddies, it is important to keep in mind that negative reinforcement could make the student look dangerous, which can be troubling in the long term. According to Seth Slater, Director of Technology for the Northwest Allen County School District, it's more important to encourage a student to use their skills for good and provide valuable insight on network security.

"I think there's a benefit there," Slater adds. "We had a stern conversation with the student, and we involved his father, who was aware of the situation." While the student hacker does have access to certain tools that are otherwise restricted to others, the student in exchange provides insight that helps an IT department fortify not just security measures to the system, but also confidential data that could have dire consequences if compromised. Slater continues to add that the outside point of view helps their IT team rethink some of the historical practices that school districts traditionally have for

Education Technology (EdTech) practices. Such practices include the way school accounts provide usernames and ID numbers to how password resets are done.

Some experts believe there should be a strong focus on making sure that the student is not perceived as a threat. Tim Tillman, CTO of Chesterfield County Public Schools believes his time as a student hacker fostered his interest in helping school staff look at security practices in a different way. By the time he was a high school graduate, he was offered a job working at the very same school that he attended. “I was given the opportunity to expand my knowledge and to explore what prompted my love of my career.” Tillman believes that students that start hacking school networks are not interested in causing any damage. “Most of what the K-12 environment would call a student hacker usually turns into someone who's trying to bypass a system. They're trying to bypass a content filter so they can watch YouTube or get the content that is restricted from them. In my position here I haven't really run across anyone yet that we have found any way that could damage our network, most of what kids are doing is trying to get to content because they're bored.” There is a potential opportunity to utilize that boredom and engage with students that is both conducive to their learning environment, in addition to fortifying it. By encouraging student hackers to share their knowledge with teachers and administrators, it gives these students a chance to return a learning opportunity to staff and faculty.

# Appendix 2

## Dungeons and Dragons and Data Breaches: Using Fantasy Games for Real Training

For those who are not familiar, Dungeons and Dragons (D&D) is a tabletop role-playing game (RPG) that has been around for over 40 years. In D&D, players take on the role of fictional characters in a fantasy world and use their imagination and problem-solving skills to navigate through various challenges.

While D&D may seem like child's play, there is actually a lot that can be learned from playing the game, especially when it comes to incident response planning. Tabletop RPGs can be used to facilitate incident response planning exercises and help prepare IT staff for real-world cybersecurity threats.

Amy McLaughlin, CoSN Cybersecurity SME, CISSP and experienced RPG gamer avidly incorporates these games with IT experts, stating that her approach to cybersecurity "The approach I use to running table-top cybersecurity  incident response scenarios is heavily based on my experience running and playing in RPGs such as D&D, Cyberpunk, and others. RPG adventuring parties require teamwork, communications, and specialized skill sets to respond to and resolve challenges and address adversaries in the game setting. These are the same collaborative team work approaches needed to successfully navigate incident response."

With the increasing number of cyberattacks and data breaches, it is more important than ever for organizations to have a robust incident response plan in place. An incident response plan is a set of procedures that an organization follows when responding to a security incident. Establishing an incident response plan is similar to creating a game plan for a tabletop RPG. Just as a party of adventurers needs to have a plan for how they are going to defeat the dragon, an organization needs to have a plan for how they are going to respond to a security incident.

Tabletop RPGs can be valuable for incident response planning for a number of reasons. One of the biggest benefits is that they can help to create a common language and understanding among the incident response team. In a tabletop RPG, each player has a

specific role to play and there is a clear division of labor. This is similar to an incident response team, where each member has a specific role to play in the response.

By playing a tabletop RPG, incident response team members can get a better understanding of the roles and responsibilities of each team member. This can be especially helpful in a large organization where the incident response team is spread out across different departments. McLaughlin elaborates that the RPG approach allows IT teams the opportunity to take on and practice roles they don't engage in. “For example, the primary information security team member may not always be available to lead response to an incident. Having other team members take the lead role in an incident response tabletop builds skills and experience being in this role."

There are a number of ways that tabletop RPGs can be used to facilitate incident response planning. One way is to use the game to create a mock incident. This can be done by creating a scenario based on a real-world incident or by coming up with a fictional incident. Mock incidents can be used to test an organization's incident response plan and procedures. They can also be used to identify gaps in the plan or areas where the procedures need to be improved.

Another way to use tabletop RPGs for incident response planning is to use them as a training tool. There are a number of incident response-themed RPGs that have been created specifically for this purpose. These games can be used to teach incident response team members how to identify and respond to different types of incidents.

There are a number of benefits to using tabletop RPGs for incident response planning. One of the biggest benefits is that they can help to bring a serious issue to a more approachable level. By using a game to simulate a real-world incident, incident response team members can get a better understanding of what they need to do without having to experience a real incident. This can be especially helpful for higher-level supervisors who may not be as familiar with incident response procedures.

Another benefit of using tabletop RPGs for incident response planning is that they can help to build teamwork and communication skills. This is because incident response team members need to work together to solve the problem.

Tabletop RPGs can be a valuable tool for incident response planning. They can help to create a common language and understanding among the incident response team, build

teamwork and communication skills, and bring a serious issue to a more approachable level. Any team looking for ideas for incident response tabletop exercises can look to CoSN's online Cybersecurity Leadership Game launched in March 2022. The game contains many incident response scenarios that can be used in planning a tabletop event.

# Appendix 3

## Low-to-no-cost Practices for Safer Networks
## *Observations from CoSN Peer Reviews*

When implementing more robust cybersecurity practices in an organization, many individuals imagine replacing costly electronics with their more expensive models. The correlation between "technology" and "expensive" tends to make school districts very cautious when investing into their IT department, because it can understandably be a barrier for many school districts. While some of these principles may be common sense to many CTOs, the CoSN Peer Review has revealed that these principles are not always achievable in underfunded districts. According to the 2022 Ed Tech Leadership Survey, budget constraints and lack of resources remain the number one challenge for district IT leaders.

It can also be exponentially difficult when a school district's network infrastructure needs to address students in rural or exurban areas such as Fauquier County, VA. According to Louis MacDonald of Fauquier County Schools, "It is an interesting dilemma between urban and rural location. In an urban setting there are potentially more resources that lower economic families can seek out that they can't in a more rural one." Fauquier County's School Division acknowledged that remote learning has highlighted an existing digital equity gap that exists in many school districts across the nation. As a result, some networking strategies start looking very costly.

Even if a school district received an infinite budget for the latest technology, that argument only holds up to a certain point. As a result, even if an organization takes the necessary steps to keep a school network up-to-date, sometimes the most innovative solutions are the simplest and cheapest ways to keep everyone safe and secure. There are many low or no cost practices that a school can utilize to establish a safer IT presence.

First, the techniques that do not cost anything are probably the most important. An extra step that makes private information harder to access results in easier to secure data. For example, staff and faculty should log off and "lock" accounts on any school equipment after school working hours. Inactive users logged on to the school intranet should be automatically logged out. Open and unlocked accounts can be operated by anyone with access to the computer, even when an employee is away from their machine. Any email

correspondence coming from outside of the school domain should come with an extended level of caution. Emails outside of the school domain can better conceal themselves as phishing emails since additional steps need to be taken to create those email addresses. These small details, when compounded together, result in a more robust network. But this user mentality is unique because it does not require any cost of training or technology. Additional safety checks, especially around technology, never become obsolete.

Regardless of your budget, all school staff should have at least a minimal understanding of the hardware and software they work with regularly. Likewise, all users must dedicate time for their hardware to download and install updates. Users need to allot time scheduled by their IT department to receive firmware updates, updated antivirus definitions, and password changes to prevent the possibility of security vulnerabilities. Finally, while mindful practices can help a user avoid cyber-attacks, it is important never to underestimate a hacker's mentality.

In conclusion, while no organization has an unlimited budget, implementing smart practices can lead to better security. Much like the adage, a ship is only as good as the people who serve on it. These simple techniques implement more preventative steps in a network than the most expensive hardware installations could ever achieve alone. If schools focus more on the proper practices, they reduce the likelihood of cyber-attack.

| **Some Potential Safer Practices for Networks** | | |
|---|---|---|
| **Practice** | **Cost Level** | **Key Points** |
| Adding Safety Checks and Protocols to Pre Existing Controls | none | • Free and Future-proof ☺<br>• No technical training needed. |
| Software Updates to Existing Equipment | none to $ | • Almost always free, with some updates (such as antivirus software and OS) being iterative purchases.<br>• Some devices that lose official support from the manufacturer still can receive homebrew updates from an independent community |
| Subscription-based & "Freemium" Software | $ to $$$ | • Scalable costs allow schools of different budgets to pay for |

| | | |
|---|---|---|
| | | what they need.<br>● Schools with smaller budgets can skip on extra features to save on costs.<br>● The Freemium model depends on access to student data, and this needs to be a consideration. |

# Appendix 4

## The Potential Risks Associated with End-of-life (EOL) Devices

While some of these principles may be common sense to many CTOs, the CoSN Peer Review has revealed that ensuring all devices are kept up to date is not easily achieved in underfunded districts and those districts that are dependent on external governance policies that may depend on approval by the general public in the form of a bond issue. Budget constraints and lack of resources remain the number one challenge for district IT leaders[8].

As hardware innovation ramps up exponentially, school districts must grapple with the question of how to manage their technology sustainably and securely, especially when their equipment is at the risk of becoming outdated in a matter of just a few years. When hardware and software reach the end of their life cycles, they become increasingly vulnerable to cyberattacks. This is because manufacturers no longer provide security updates or support for these products, leaving them open to exploitation by malicious actors.

In 2020 alone, 53 chromebook models will no longer receive updates[9]. More brands are giving set expiration dates to their still-capable hardware. School districts rely on devices such as chromebooks for affordability and wide compatibility to education oriented web applications. Giving these deadlines forces schools to decide between their limited budgets and their security.

End-of-life hardware presents unique risks to school districts in terms of cybersecurity. This is because outdated software vulnerabilities are no longer patched by the device's manufacturing company, leaving the door open for malicious actors to exploit them. In addition, end-of-life equipment is often unsupported by the manufacturer in both hardware and software, meaning that school districts will have to find other ways to keep their systems secure. Once hardware and software reach the end of their life cycles, they are no longer supported by manufacturers. This means that if something goes wrong with the product, there is no one to turn to for help.

---

[8] CoSN 2022 EdTech Leadership Report
[9] What is a Chromebook's lifespan?, PC Week, August 2020

One of the most important security measures for any piece of technology is to keep it up-to-date with the latest security patches and updates. However, when hardware and software reach the end of their life cycles, manufacturers no longer provide these updates, leaving devices vulnerable to attack. If an operating system no longer receives updates this year, it's a sitting duck the next.

Fortunately, there are a number of things that school districts can do to mitigate the risks associated with using end-of-life hardware. One way to mitigate the risks associated with end-of-life hardware is to have a sustainability plan in place. This plan should include a reasonable cycle for replacing and repairing equipment. In addition, the long-term costs of a school district being vulnerable to a cyber attack should be considered. One way to offset the costs of new technology and reduce e-waste is to sell old hardware to resellers where the hardware can be refurbished.

With the right sustainability plan in place, school districts can balance the need to keep their systems secure with the need to reduce e-waste. By considering the long-term costs of using end-of-life hardware, school districts can make the best decision for their students, staff, and community.