CYBER 101 FOR K-12

A GUIDE FOR SUPERINTENDENTS, ADMINISTRATORS, AND INFORMATION TECHNOLOGY DIRECTORS

STEPHEN CHAPEL & JESSENIA VILLANUEVA| DATA DIVERS LLC |
APRIL 2024

INDEX

Introduction:
K-12 education is one of the most targeted industries, surpassing other sectors such as construction, government, and healthcare. Yet schools only show moderate preparedness according to CIS' Nationwide Cybersecurity Review scoring a 3.55 out of 7. Cyberattacks during the 2022-23 school year frequently left schools having to cancel classes or close completely as a result of disruptive building operations and classroom technologies. Loss of learning following cyber attacks ranged from 3 days to 3 weeks, and recovery time can take anywhere from 2 to 9 months.

Roughly 80% of K-12 schools are impacted by ransomware attacks, with an average payment of $1.2 million in exchange for returning the data unharmed or exposed. According to a 2023 study, K-12 schools have leaked over 5.3 million records since 2005.

The Urgent Need for Cybersecurity in K-12:
Recently, Minneapolis Public Schools were hit by what experts describe as one of the most devastating cyber attacks ever in which hackers stole district data, including files where children were identifiable, and then demanded the district pay a ransom for it. When district officials refused, the hackers released the data online, affecting over 105,000 people. It included Social Security numbers, campus security technology details, blueprints of district school buildings, and information about sexual assaults and psychiatric holds.

Just a few months later, A Connecticut school district lost $6 million to hackers. The hackers appear to have gained access in late May 2023 to the email account of the school system's chief operating officer and began to monitor conversations among the school officials, vendors and the city's finance office. The hackers then impersonated the school official and vendors in order to divert the school's money to fraudulent accounts.

Understanding the Target:
One reason for the increase in attacks is that hackers have realized school systems are data rich and cyber poor.

School systems often contain sensitive information concerning their students and their student's family dynamic. This could include attendance records, medical records or more personal information that could be used to steal a child's identity. Cyber criminals have even obtained data concerning sexual assaults and psychiatric holds which can leave long lasting effects on the victims. A main contributor to this information being exploited is that K-12 organizations often do not have the resources or tools in place to defend against such attacks.

They often have older computer systems, rely heavily on technology, and more than likely don't have cyber security experts on staff. A recent survey showed that 49% percent of K-12 schools have only 1-5 cyber or IT employees, only 1/3rd of school districts have a full-time employee dedicated to cybersecurity, and on average schools are spending only about 8 percent of their IT budgets on cybersecurity. This underinvestment makes their digital infrastructure less secure, leaving them vulnerable to hackers.

Additional Constraints:
Resource constraints go hand in hand with as the very reason K-12 schools are highly targeted. Most school districts are doing a lot with a little and resource shortfalls can be a major constraint to implementing effective cybersecurity programs. Some additional constraints can include the following:

- Limited Access to Training and Education
- Complex Regulatory Environment
- Insufficient Awareness and Support
- Limited Collaboration and Information Sharing
- Inadequate Incident Response Capabilities
- Insufficient Access Controls and Monitoring
- Rapidly Evolving Threat Landscape

Addressing these resource constraints requires a coordinated effort involving school administrators, educators, parents, students, government agencies, and cybersecurity organizations. Collaboration, advocacy for increased funding and support, leveraging free or low-cost resources, and prioritizing cybersecurity within the school community can help mitigate these constraints and enhance the effectiveness of K-12 cybersecurity programs.

Steps to Strengthen Cybersecurity:

1. **Assess Current Capabilities:** Begin by assessing the existing expertise and resources within your school community. Identify staff members with relevant IT or cybersecurity experience, as well as any existing policies, procedures, or technologies related to cybersecurity.
2. **Identify Key Roles and Responsibilities:** Determine the specific roles and responsibilities needed for your cybersecurity team. This may include positions such as a cybersecurity coordinator, IT administrator, data protection officer, and incident response manager.
3. **Provide Training and Professional Development:** Invest in training and professional development opportunities for staff members interested in cybersecurity roles. Offer courses, workshops, and certifications to build their skills and expertise in areas such as network security, data protection, incident response, and compliance.
4. **Establish Clear Policies and Procedures:** Develop clear policies and procedures governing cybersecurity practices within the school, including acceptable use policies, data protection guidelines, incident response protocols, and compliance with relevant regulations such as FERPA and CIPA.
5. **Implement Security Technologies:** Deploy appropriate security technologies to protect school networks, systems, and data. This may include firewalls, antivirus software, intrusion detection systems, encryption tools, and security awareness training platforms.
6. **Promote a Culture of Cybersecurity Awareness:** Foster a culture of cybersecurity awareness among students, staff, and parents. Provide regular cybersecurity training and awareness campaigns to educate the school community about online risks, safe internet practices, and responsible technology use.
7. **Encourage Collaboration and Communication:** Foster collaboration and communication among members of the cybersecurity team, as well as with other school staff, administrators, and external stakeholders. Establish channels for reporting security incidents, sharing information, and coordinating responses to cybersecurity threats.
8. **Monitor and Evaluate Performance:** Continuously monitor and evaluate the performance of

your cybersecurity team and cybersecurity initiatives. Track key metrics such as incident response times, compliance with policies, and effectiveness of training programs to identify areas for improvement and ensure ongoing success.

9. **Stay Informed About Emerging Threats:** Keep abreast of emerging cybersecurity threats and trends in the education sector. Stay informed about new technologies, vulnerabilities, and best practices in cybersecurity to proactively address potential risks and adapt your security strategies accordingly.

Training and Education:

All personnel at every K-12 organization should be formally trained to understand the organization's commitment to security, what tasks they need to perform (like enabling MFA, updating their software and avoiding clicking on suspicious links that could be phishing attacks), and how to escalate suspicious activity.

While staff training may focus more on technical aspects and compliance with organizational policies, student training emphasizes practical strategies for staying safe online and promoting responsible digital citizenship.

Aspect	Staff Training	Student Training
Audience	School faculty, administrators, and staff	K-12 students
Objectives	Enhance understanding of cybersecurity policies and procedures, improve data protection practices, and develop incident response skills	Foster awareness of online risks, promote safe internet practices, and encourage responsible digital citizenship
Focus Areas	Data protection, phishing awareness, incident response, network security, device security	Safe internet practices, social media safety, password security, cyberbullying prevention, digital citizenship
Technical Complexity	May include more technical topics relevant to school networks and systems, such as network configuration, access controls, and software updates	Emphasizes basic cybersecurity concepts and practical strategies tailored to students' digital activities and online interactions
Compliance	Emphasizes compliance with school-specific cybersecurity policies, regulations (e.g., FERPA), and industry standards	Promotes adherence to school rules and acceptable use policies, with a focus on responsible behavior and ethical considerations
Training Methods	May involve in-depth workshops, online courses, hands-on exercises, and simulations tailored to staff roles and responsibilities	Incorporates interactive activities, age-appropriate games, videos, and discussions to engage students and reinforce learning
Incident Response	Staff training typically includes detailed protocols and procedures for reporting cybersecurity incidents, collaborating with IT/security teams, and mitigating risks	Students are taught basic incident reporting procedures and encouraged to seek help from trusted adults or school personnel in case of cyberbullying, online harassment, or other safety concerns
Continuous Education	Encourages ongoing professional development, certification programs, and participation in security awareness initiatives to stay updated on evolving threats and best practices	Promotes continuous learning and reinforcement of cybersecurity principles through periodic refreshers, guest speakers, and integration into curriculum subjects like computer science or digital literacy
Communication	Highlights the importance of clear communication and collaboration between staff members, IT/security teams, and school leadership to address cybersecurity challenges effectively	Encourages open dialogue between students, parents, teachers, and school counselors about online safety, cyberbullying prevention, and responsible technology use

Tools for the Cybersecurity Team

Implement Multi Factor authentication (MFA)

MFA makes it more difficult for cyber threat actors to gain access to networks and information systems if passwords or personal identification numbers (PINs) are compromised through phishing attacks or other means. It requires two or more factors to gain access to the system. Each factor must come from a different category below:

- Something you know
    - Password, or pin
- Something you have
    - Smart card, one-time password devices
- Something you are
    - Fingerprints, facial recognition, voice pattern

With MFA enabled, if one factor, such as a password, becomes compromised, unauthorized users will be unable to access the account if they cannot also provide the second factor. This additional layer ultimately stops some of the common malicious cyber techniques, such as password spraying.

Identify and Fix Known Security Flaws
Prioritize remediation of known exploited vulnerabilities that are listed on the Cybersecurity and Infrastructure Security Agencies (CISA's) Known Exploited Vulnerabilities (KEV) catalog. You can either sign up for recurring updates when new vulnerabilities are added, or use a third-party service that automatically identifies the presence of vulnerabilities on CISA's KEV Catalog or alternative catalogs.

Perform and Test Backups
Identify data that is critical to continued operations of your K-12 organization and employ a backup solution that automatically and continuously backs up your business-critical data and system configurations.
Regular backups protect against ransomware and malware attacks. Use on-site and remote backup methods to protect vulnerable information. Prioritize backups (based on the importance of the information) and have a schedule of what to bring back online when so that your business can still function during a cyberattack. Test your backup strategy before you need to use it to make sure you have full read-back verification, a method of preventing errors when information is relayed or repeated in a different form in order to confirm its accuracy.
Backups should be stored in a secure location. Periodically test your ability to recover data from backups.

Minimize Exposure to Common Attacks
Malicious cyber actors continuously scan organizations to identify vulnerabilities and execute damaging intrusions. Every K-12 organization should ensure that their Internet-connected assets are up-to-date and free from exploitable conditions. A few tools that can help achieve this is performing vulnerability scans, reducing internet attack surfaces by segmenting your network and implementing appropriate access controls which can include firewalls, routers, access control lists (ACLs), virtual LANs (VLANs), and other network security mechanisms.

Minimize your Attack Surface
By shutting off search functionality and controlling access to online resources for students and staff we can limit the attack surface of our K-12 organization

1. Blocking Malicious Search Results: Schools may use web filtering and firewall solutions to block access to websites known to host malware or phishing attempts. "Shutting off search" could involve configuring these filters to prevent users from accessing search results leading to such malicious websites.
2. Restricting Access to Certain Search Engines: Schools might choose to limit access to specific search engines known for privacy concerns or a higher likelihood of returning inappropriate results. For certain search engines, schools can control the tools students and staff use for online research.
3. Monitoring and Reporting: Instead of completely blocking search functionality, schools may opt to monitor search activity for suspicious or inappropriate behavior. This could involve implementing logging and reporting mechanisms to track search queries and identify potential

cybersecurity threats or policy violations.

Incident Response Planning

Every K-12 organization should have an Incident Response Plan that spells out what the organization needs to do before, during, and after an actual or potential security incident. It should be approved by the senior official in the organization and reviewed quarterly, and after every security incident or “near miss”. Below are the four main components of an incident response plan:

Preparation

- Preparation involves training personnel and the gathering of information, tools, and resources.
- School officials must first determine what a cyber incident means for their organization, i.e. anything that violates or poses a threat and/or is in violation of its policies and procedures. IE misuse of district technology resources by staff or students.
- Determine who is part of the IR team and what their role is during an incident
- Identify key contacts and resources
- Prepare your communications/PR team for cyber incident communications.

Detection & Analysis

- Determining the potential scope and impact of a cyber incident helps prioritize response and recovery efforts. It is important to prepare for common K-12 incidents such as brute force attacks and phishing email compromise.
- Monitor for potential incidents and understand the possible sources and precursors of potential incidents ie unexpected patching of systems or firewall alarms
- IT staff should be trained on the steps to declare a potential cyber incident and invoke the Incident Response team upon discovering a potential incident. The team should gather and document evidence to assist with incident response and fulfilling legal obligations.

Containment , Eradication, and Recovery

- Based on the information gathered during the prior stage, thoroughly eradicate malware and vulnerabilities - and restore normal operations.
- Contain the incident: Block compromised systems from communicating with other devices or with attackers.
- Eradicate the threat: After ensuring evidence has been preserved for legal and insurance purposes, eliminate all traces of the incident.
- Recovery: Repair, restore, rebuild, or replace systems that were taken offline or otherwise affected by the incident.

Post Incident Activity

- Document and share lessons learned from incident response to resolve deficiencies and strengthen the security posture of your organization, as well as peer institutions.
- A comprehensive assessment must be prepared and shared with appropriate parties, including executive leadership, and changes should be implemented based on the learned lessons.

Free Resources for K-12 Organizations

1. The SLCGP provides $1 billion over 4 years for state, local, and territorial (SLT) governments funding to support efforts addressing cyber risk to their information systems. And while the funding is granted directly to the State Administrative Agency, publicly funded K-12 schools are eligible to receive sub-award money.
2. The Cybersecurity and Infrastructure Security Agency has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This living repository includes cybersecurity services provided by CISA, widely used open-source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community. CISA RESOURCES AND DHS GRANTS
3. K–12 organizations should expect the technology used for core educational functions like learning management and student administrative systems to have strong security controls enabled by default for no additional charge. Ensure that vendors do not charge more for security features like MFA and logs. As you deploy products be sure to review the product's "hardening guide". A hardening guide is a set of steps to make the product less dangerous.

Attack Examples

Data breach

- Illuminate Education
  https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html
- (CPS) Chicago Public Schools
  https://chicago.suntimes.com/education/2022/5/20/23132983/cps-public-schools-data-breach-students-employees-records-battelle-kids

Ransomware

- New Haven Conn. ($6mil)
  https://www.k12dive.com/news/cyberattack-New-Haven-schools-6-million/691284/

DDos

- Miami-Dade County Public Schools (2020)
  https://www.spiceworks.com/it-security/network-security/news/ddos-attacks-plague-miami-dade-county-public-schools/
- Miami-Dade 16 year old admits DDOS attack - foreign threat actors
  https://www.local10.com/news/local/2020/09/03/superintendent-miami-schools-platform-also-targeted-by-foreign-interference/

References:

https://www.forbes.com/sites/frederickhess/2023/09/20/the-top-target-for-ransomware-its-now-k-12-schools/?sh=146e72d7563f

https://www.npr.org/2024/03/12/1237497833/students-schools-cybersecurity-hackers-credit#:~:text=While%20it's%20hard%20to%20know,more%20than%20doubled%2C%20to%20108.

https://www.edweek.org/technology/school-cyberattacks-explained/2022/02

https://www.npr.org/2024/03/11/1236995412/cybersecurity-hackers-schools-ransomware

https://managedmethods.com/blog/cyber-attack-impacts/
Data Rich - Cyber Poor
https://www.govtech.com/security/data-rich-resources-poor-cis-report-targets-gaps-in-k-12-cyber

Known Exploited Vulnerabilities Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog?page=0

K-12 School Service Provider Pledge to Safeguard Student Privacy
https://web.archive.org/web/20141008223425/http://studentprivacypledge.org/?page_id=45

Cybersecurity Resources for K-12 Schools and School Districts
https://www.schoolsafety.gov/sites/default/files/2024-02/SchoolSafety.gov%20Cybersecurity%20Resources%20for%20K-12%20Schools%20and%20School%20Districts%20Infographic_February%202024_508C.pdf