Cybersecurity for Your School

THE CHARTER SCHOOL CYBERSECURITY GUIDE

In partnership with Software MSP

Grow Schools

For charter schools, it's about staying ahead and meeting the evolving needs of your school. Having the proper cybersecurity protection in place is essential—which means upgrading and modernizing systems and ensuring robust security measures.

A secure digital environment safeguards sensitive data and protects against potential risks, helping your school to remain competitive, relevant, and secure within the ever-evolving digital landscape.

This guide is designed to help build your school's cybersecurity and keep all digital spaces safe and sound. You'll find easy-to-follow recommendations and best practices aligned with the National Institute of Standards and Technology (NIST) Cyber Security Framework.

The information in this guide comes to you in collaboration with the team at SoftwareMSP, providing technology solutions to schools across the country.

Table of Contents

Why Cybersecurity Matters for Your School

Why Cybersecurity Matters for Your School

Your school handles a vast amount of sensitive data–including student records, financial information, and employee information. Cybersecurity measures help prevent the unauthorized disclosure of personally identifiable information (PII) and maintain compliance with student privacy laws, such as the Family Educational Rights and Privacy Act (FERPA).

Cyberattacks–like ransomware or distributed denial-of-service (DDoS) attacks–can disrupt school operations and negatively impact student learning. Robust cybersecurity measures help safeguard intellectual property from theft, unauthorized access, or infringement. By fostering a culture of cybersecurity, charter schools can empower their students and staff to make informed decisions, protect themselves online, and contribute to a safer digital environment.

How Common Are Cyberattacks Against Schools?

Cyber attacks are increasing, and schools are becoming targets more often.

Why schools? In an article for Forbes, Frederick Hess points out that online learning has only made things worse in recent years. Hess spoke with Doug Levin, co-founder of the K12 Security Information eXchange (K12 SIX), who stated that there have been more than 1,300 publicly disclosed incidents since 2016. Levin told Hess it comes down to money: "Schools manage more than enough money to capture the attention of cyber criminals."

Alyson Klein echoes these words in EdWeek: the problem is only increasing as schools rely more and more on technology. As for who is carrying out these attacks, it depends on the case: anyone from bored students to offshore criminals can find a reason to attack a school's files.

Types of Cyberattacks

Ever gotten an email from someone claiming you'd won a cash prize? Or maybe a text message from someone pretending to be a company your know, like Netflix? These are forms of phishing, and they represent just one way of attempting to secure private data. Phishing is only one kind of cyberattack.

Here's a look at the most common ones.

PHISHING

Phishing is a form of fraudulent solicitation via email or on a website. It can prompt someone to enter personal information while masquerading as a trustworthy entity.

DATA BREACH

Often called simply a "hack," a data breach is when an unauthorized person gains access to sensitive, confidential, or protected information stored by your school.

RANSOMWARE

A ransomware attack is when cyber criminals use malicious software to break into a school's network and encrypt the data–so your school can no longer access it. As the word "ransom" suggests, they say they will only release the files back to the school if a certain amount is paid first. According to CNN, schools with limited cybersecurity measures are often the most vulnerable to ransomware.

DENIAL-OF-SERVICE ATTACK

This is known as a "crash"–when cybercriminals infiltrate a network with so many requests it stops responding. This blocks those that need the network from being able to use it.

PRANKS, INVASIONS, AND HACKTIVISM

Online learning has given rise to pranks like "Zoombombing," where an outside person gets into an online class and disrupts it with inappropriate–or even hateful– messages or images. Such pranks–which seem to stem solely from the desire to disrupt– can also occur in parent meetings, online performances, and over email. "Hacktivism" involves similar tactics and protests against school policies or changes.

What's the Impact?

WASTED TIME

Often, schools must close during a cyberattack. According to a U.S. Government Accountability Office (GAO) survey[1], "loss of learning following a cyberattack ranged from 3 days to 3 weeks, and recovery time could take anywhere from 2 to 9 months."

WASTED MONEY

The GAO survey reports losses[1] due to cyberattacks are significant. They include replacing computer hardware and enhancing cybersecurity to prevent future attacks.

LEARNING LOSS AND OTHER HARM

Cyberattacks disrupt learning with their impact on students, their families, and teachers. If systems are down, teaching and record-keeping cannot be conducted as planned. A 2020 GAO study[2] found that breached grades, bullying reports, and social security numbers left students "vulnerable to emotional, physical, and financial harm."

[1] *As Cyberattacks Increase on K-12 Schools, Here Is What's Being Done.* https://www.gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done. December 2022.

[2] *Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm.* https://www.gao.gov/products/gao-20-644. September 2020.

Make Your Cybersecurity Plan

Make Your Cybersecurity Plan

The number of cyberattacks against schools is staggering: GAO reports that in 2020 there were 1,196,000 ransomware attacks alone. (Their reports include a list of the most notable incidents over the last few years, which you can find here: "As Cyberattacks Increase on K-12 Schools, Here is What's Being Done.") Many law and policymakers are calling for better support around cybersecurity for schools.

The good news is: you can mitigate the risk to your school.

STEP 1
Identify and Protect

To improve your school's cybersecurity, it's essential first to identify what needs to be protected. Start by identifying the most critical processes and assets within your school. These could be systems that handle student data, financial transactions, or other information essential to your school's operation.

TIP Your school's student information system, which stores and manages student records, grades, and attendance, is a critical asset that needs protection.

Once you have identified the critical assets, assess their associated risks. This involves evaluating potential vulnerabilities and threats that could compromise the security of these assets.

STEP 2

Create a Comprehensive Inventory

Create and maintain a comprehensive inventory of all hardware, software, and storage locations where sensitive data is stored. This includes servers, databases, computers, and other devices used in your school's operations.

TIP Keep track of all computers used by staff and students, ensuring that their security software is up-to-date and regularly monitored.

STEP 3

Initiate Regular Monitoring, Updates, and Record-Keeping

Ensure that your school's networks, computers, and systems are regularly monitored and updated. This helps identify potential security issues and ensures you stay ahead of emerging threats. You'll also want to document and analyze your critical assets' threats, vulnerabilities, and risks. This documentation helps in understanding potential weak points and developing effective mitigation strategies.

TIP Maintain a log of attempted cyber-attacks on your school's systems, which helps identify patterns and areas that require extra protection.

STEP 4

Implement Protective Measures

Implement protective measures such as firewalls, intrusion detection systems, data encryption, and access controls to safeguard your critical assets. Use multi-factor authentication for staff accessing sensitive data, adding an extra layer of security beyond passwords.

Features of a Robust Cybersecurity Framework

Features of a Robust Cybersecurity Framework

Here's what to consider as you design a robust and comprehensive cybersecurity plan for your school.

DATA MANAGEMENT POLICY

Data management practices are essential for maintaining the confidentiality and integrity of sensitive information. A comprehensive data management policy should cover data collection, storage, access, and usage. It should detail how data should be classified based on sensitivity and specify the appropriate security measures for each category. Regular audits and reviews of data management practices ensure compliance and identify areas for improvement.

TIP Your school's data management policy categorizes data into public, internal, and confidential levels. Confidential data, such as student records, is encrypted during transmission and storage, and access is restricted to authorized personnel only.

ENCRYPT AND BACK UP SENSITIVE DATA

Keep sensitive information confidential by encrypting it on computers and sending it to others. Encryption ensures that even if data is intercepted, it remains secure and unreadable to unauthorized parties. Regular backups are essential, and offline backups can safeguard against ransomware. Automated backups and redundancy features further protect data from hardware failures or loss.

REGULARLY UPDATE SYSTEMS AND SOFTWARE

Keep your systems and software up-to-date by automating updates whenever possible. This helps fix vulnerabilities and ensures your school's IT infrastructure stays secure and reliable.

SECURE DISPOSAL OF ELECTRONIC FILES AND OLD DEVICES

Properly disposing of electronic files and old devices is crucial to prevent data leakage. Sensitive data may reside on outdated devices or in no longer needed files, making them potential targets for unauthorized access. Implementing a secure data disposal process involves using data erasure methods, physically destroying storage media, and adequately recycling electronic devices.

TIP Collaborate with a certified electronic waste recycler to ensure that old devices are wiped clean of data or physically destroyed before recycling.

ROLES AND RESPONSIBILITIES FOR EMPLOYEES AND VENDORS WITH ACCESS TO SENSITIVE DATA

Defining clear roles and responsibilities is critical in maintaining the security of sensitive data. Each employee should have a unique account, and adding multi-factor authentication (MFA) provides an extra layer of protection. Limit user access to only what's necessary for their specific roles.

Each employee and vendor with access to sensitive information should have a well-defined understanding of their responsibilities regarding data protection. This involves adhering to specific guidelines, using secure authentication methods, and promptly reporting suspicious activities. By creating a culture of data responsibility and accountability, your school can minimize the risk of data breaches and unauthorized access.

TIP Ensure your school has a clearly defined IT policy outlining the access levels and data handling responsibilities of teachers, administrators, and third-party vendors. Then be sure employees receive regular training on data protection practices to ensure they understand their roles in maintaining data security.

CREATE AN AWARENESS AND TRAINING PROGRAM

Develop a Cyber Security Awareness and Training Program for your staff. Regular training sessions will educate employees about current threats and safe practices, empowering them to contribute to data security actively. Each employee should understand your data management policies and their role in promoting safe practices.

The program should cover:

- **Awareness:** Help employees understand the importance of security and the potential risks to the organization. Everyone should recognize their responsibility in preventing cyberattacks and protecting sensitive data.
- **Protocols:** Employees should know best practices for accessing and protecting personally identifiable information (PII), safeguarding data confidentiality, and preserving system security.

Creating Your Incident Response Plan

Creating Your Incident Response Plan

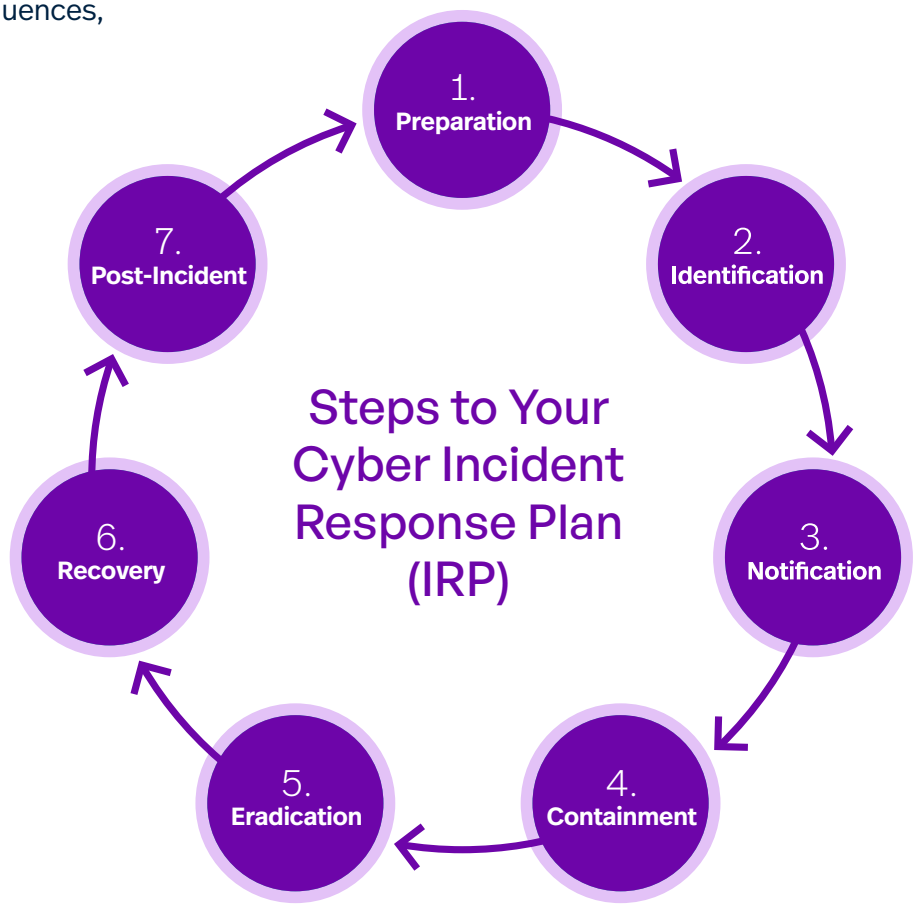
Even schools with the best safeguards in place can still become victims of a cyberattack. The threat landscape is constantly evolving, and cybercriminals are always looking for new ways to exploit vulnerabilities. It's essential to have a plan in place if your school becomes a target.

Having a well-defined and practiced Incident Response Plan is essential. The biggest thing to consider is that time is of the essence when a cyberattack occurs. A swift and coordinated response can significantly reduce the attack's impact and help prevent further consequences, setbacks, and learning loss.

Identify and Train Your Incident Response Team (IRT)

The IRT is a group responsible for coordinating and executing your school's response when a cyber incident occurs. Their expertise and preparedness are crucial for a well-coordinated response.

- **Establish Roles and Responsibilities:** Determine the critical roles required for effective incident response, such as Incident Response Manager, IT specialists, legal representatives, communications personnel, and other stakeholders. Ensure that all IRT members undergo cybersecurity awareness training.
- **Identify Subject Matter Experts (SMEs):** Identify individuals with expertise in various areas, such as IT security, forensics, legal, compliance, public relations, and risk management. SMEs bring specialized knowledge to address specific aspects of an incident.
- **Outsource:** Don't have the staff for an IRT? Consider partnering with an external team of experts.



IDENTIFICATION

Assess the impact and severity of the incident. Your school should have monitoring systems to identify unusual activities or potential breaches. Proactive monitoring can help detect attacks in their early stages, giving the response team a head start in containing and mitigating the impact.

NOTIFICATION

Create a well-defined communication plan that outlines who needs to be informed, what information needs to be shared, and the communication channels to be used. A severe incident may compromise company communication resources (email, phone system, etc.). Establish primary and alternate methods of communication using external infrastructure. These communication methods will be noted on the Incident Response Team (IRT) member contact list, ensuring everyone can access specific communication channels during an incident. The IRT and all individuals involved in resolving the incident will be directed on which communication method to use, ensuring clear and coordinated communication throughout the response.

CONTAINMENT

Once an attack is confirmed, the focus should be on containing the threat to prevent it from spreading further. This may involve isolating affected systems, disabling compromised accounts, or blocking malicious activities.

ERADICATION

Depending on the nature and scale of the attack, it may be necessary to engage external cybersecurity experts or Computer Incident Response Teams (CIRTs). These experts can provide specialized knowledge and support to the school's IRP in effectively handling and eradicating the incident.

RECOVERY

Accurate and thorough incident documentation is crucial for post-incident analysis, learning, and potential legal actions. The Incident Response Team (IRT) should record all actions taken, findings, and responses during the incident. After containing the threat, the focus shifts to recovery. Schools should restore affected systems and services to normal operation as quickly and securely as possible. This may include restoring data from backups and conducting security checks. You'll also want to address any legal issues related to the cyber incident.

POST-INCIDENT

Assess the effectiveness of your IRP, identify any gaps or areas for improvement, and update the Incident Response Plan accordingly. Coordinate with external Computer Incident Response Teams and law enforcement if needed.
The timing of recovery from a cyberattack on a school can vary significantly depending on the nature and severity of the attack. Recovering from a cyber incident is a complex process that involves several factors, such as the type of attack, the extent of the damage, the availability of resources, and preparedness.

Process Phase & Approximate Timing	Process Detail Steps	Involved Parties
IDENTIFICATION (Hours)	1. Identify and confirm that the suspected or reported incident has happened and whether malicious activity is still underway. 2. Determine the type, impact, and severity of the incident by referring to Appendicies B, C, and D. 3. Take basic and prudent containment steps.	IT and any monitoring service provider
NOTIFICATION (Hours–1 Day)	4. Inform or activate the IRT, based on the severity of the incident, as outlined in Appendix D, and provide the type, impact, and details of the incident to the extent that they are known. 5. Determine the need for Subject Matter Experts (SME) to be involved in the Containment, Eradication, and Recovery processes.	IT & IRT
CONTAINMENT (Hours–2 Days)	6. Take immediate steps to curtail any ongoing malicious activity or prevent repetition of past malicious activity. 7. Re-direct public facing websites, if needed. Provide initial public relations and legal responses as required.	IRT, IT, SME's
ERADICATION (Days–Weeks)	8. Provide full technical resolution of thread and related malicious activity. 9. Address public relations, notification, and legal issues.	IT, IRT, SME's
RECOVERY (Weeks–Months)	10. Recover any business process disruptions and re-gain normal operations. 11. Address longer term public relations or legal issues, if required, and apply any constitutent remedies.	SME's & IRT
POST-INCIDENT (Months)	12. Formalize documentation of incident and summarize learnings. 13. Apply learnings to future preparedness.	IRT

Distributing and Training Your IRP

While no incident can be perfectly scripted, this plan serves as a framework for managing cybersecurity incidents, allowing flexibility to address each unique situation. Being prepared is key, as is having printed copies of your response plan accessible to everyone involved.

TIP Don't hesitate to involve your contacts at local law enforcement if you need assistance during a cyberattack.

The Ongoing Effort and How to Get Help

The Ongoing Effort and How to Get Help

Protecting sensitive data and ensuring the smooth functioning of educational programs is an ongoing effort.

As your school grows and you adopt or evolve your technology, you can create more robust protective measures to run your school without the fear of a data breach.

CHOOSING THE RIGHT PARTNER

Navigating two-factor authentication, backup data, secure logins, and technical troubleshooting can be daunting for school leaders already stretched so thin–that's when it can be helpful to reach out to an external partner to help. Selecting the right technology partner for cybersecurity solutions is vital.

As you look for a partner, make sure you're looking for the following qualities:

- Education-focused in their offerings, with familiarity with the types of systems schools use and the data they own.
- Have a Security Operations Center (SOC) for rapid response.
- Offer guidance on lessons learned to enhance future protection.

SOURCES

Federal Student Aid Cybersecurity, "Cybersecurity Incident Planning for Institutes of Higher Education"

U. S. Department of Education, Protecting Student Privacy, Cybersecurity Best Practices for Schools and Districts, https://studentprivacy.ed.gov/Security, July 27, 2023

You can get the money, resources, and know-how to create a thriving school.

WE CAN HELP WITH:

- Money to run your school
- Money to buy your school
- Kids to fill your school

Let's get started.

LIVE CHAT
growschools.com

EMAIL
hello@growschools.com

TOLL-FREE
(877) 272-1001

SOFTWARE MSP

We are grateful to the experts at SoftwareMSP for the co-creation of this guide.

Learn more about how their team can support your school's technology needs at softmsp.com/growschools or email info@softmsp.com.

Grow Schools

Helping you get where you're going.