ThreatDown™
Powered by Malwarebytes

2025 Cybersecurity Guide for Education

Contents

Introduction

Schools, colleges, districts, and education service providers are faced with one of the toughest challenges in cybersecurity.

They must operate complex networks and safeguard sensitive data in a highly regulated environment—all while managing increasingly tight budgets. And they must protect students from online harm, mitigate a significant insider threat risk, handle enormous churn in their user population every year, and cater to the widely differing needs of both students and faculty.

This combination of challenges makes educational institutions and their supply chains prime targets for ransomware gangs. IT and security staff must therefore be prepared to defend their schools and colleges against organized, well-funded and highly experienced attackers.

This easy-to-use guide is designed to help educational institutions tip the scales back in their favor. It sets out the nature of the threats they face and their overarching compliance obligations, and it provides a simple risk assessment framework, an explanation of the tools they need to protect their environment, and a 10-step recovery plan to help them prepare for a breach.

Understanding the threat

Over the last six years, the nation's schools have disclosed an average of more than one cyber incident per school day, with many more incidents likely going unreported.[i]

Attacks and data breaches disrupt learning, expose the personal identifiable information (PII) of students and staff, and are extremely costly to resolve, with the average education data breach costing $3.65 million.[ii]

The scale of these breaches can be enormous:

- In December 2024, attackers compromised over 70 million student and staff records from over 6,000 school districts in the US and Canada, by attacking PowerSchool cloud software.
- A breach at Chicago Public Schools in late 2024 exposed the personal details of "hundreds of thousands" of current and former students, including names, dates of birth, gender, student ID numbers, and Medicaid ID numbers.
- In September 2024, the Rhysida ransomware group leaked the student records of 450,000 current and former students from Utah's Granite School District after it refused to pay a $1.5 million ransom.
- More than half a million people were affected when criminals stole SSNs, payment card information, passport numbers, and medical data from the Pennsylvania State Education Association (PSEA) in July 2024.

US educational institutions are unprepared for a cyberattack

The most recent Nationwide Cybersecurity Review, which measures maturity according to the NIST Cybersecurity Framework, found that most education sectors fall below the recommended minimum maturity level of 5, and well below the maximum of 7.[iii]

Subsector	All function average
State - Education	5.23
State - Higher Education	4.60
Local - Higher Education	4.35
Local - K-12 Schools	3.45

[i] K12 Security Information Exchange (2022), The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report, https://www.k12six.org/the-report

[ii] IBM (2024), Cost of a Data Breach Report 2024, https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258.

[iii] Center for Internet Security (2024), Nationwide Cybersecurity Review: 2023 Summary Report, https://www.cisecurity.org/insights/white-papers/nationwide-cybersecurity-review-2023-summary-report.

Understanding your obligations

US educational institutions operate in a complex regulatory environment and must comply with multiple, overlapping federal and state privacy and cybersecurity laws.

Increasingly, schools and colleges must not only practice strong cybersecurity but also be prepared to demonstrate it through training, documentation, policies and reports, and through the adoption of security frameworks.

Major federal regulations affecting US schools and colleges

Regulation	K-12	Higher
Children's Internet Protection Act (CIPA) E-Rate funded schools must implement content filtering, monitoring, and policies to protect minors.	✓	
Family Educational Rights and Privacy Act (FERPA) Schools must implement policies and controls to protect students' educational records.	✓	✓
Children's Online Privacy Protection Rule (COPPA) Schools must limit collection of children's personal information and protect it from unauthorized use.	✓	✓
Gramm-Leach-Bliley Act (GLBA) Schools processing financial aid must safeguard financial information.		✓
Payment Card Industry Data Security Standard (PCI-DSS) Schools accepting card payments must secure cardholder data, encrypt transactions, and regularly monitor and test systems.		✓
Health Insurance Portability and Accountability Act (HIPAA) Schools providing healthcare services must protect students' data with encryption, access controls, and secure storage.		✓
NIST 800-171 Schools handling federally funded research data must protect CUI[1] with NIST 800-171 security controls.		✓
Cybersecurity Maturity Model Certification (CMMC) Schools with DoD research contracts must meet CMMC cybersecurity standards to protect CUI.		✓

[1] CUI: Controlled Unclassified Information.

The ThreatDown Education bundle can help educational institutions meet their compliance obligations by blocklisting applications, stopping malware and blocking malicious websites, enforcing policies, and providing transparent logging and reporting.

Prevent: A simple risk assessment

To implement an effective cybersecurity strategy that provides safety and security, and supports their compliance efforts, it is essential that schools, districts, and colleges understand the risks they face.

The following process provides a foundation for conducting a basic risk assessment. This assessment identifies critical assets, the threats they may encounter, and the potential consequences of failing to protect them.

Institutions are encouraged to document their findings thoroughly. Doing so not only demonstrates the methodology used but also allows for easier updates to the risk assessment in response to environmental changes or insights gained from security incidents.

Step	Action
1. Assets	Create a comprehensive inventory of your hardware, applications, user types, and stored data.
	Complete the actions below for each asset identified in step 1.
2. Threats	Identify the threats that could harm the asset. Threats are things like password cracking, breaches, and ransomware.
3. Weaknesses	Identify weaknesses threats could exploit to cause damage, such as software vulnerabilities or weak password policies.
	Complete the actions below for each weakness identified in step 3. In determining risk, we recommend you weigh impact more heavily than likelihood, so you are adequately prepared for rare events with a severe impact, such as ransomware.
4. Likelihood	Decide how likely it is that this weakness will be exposed.
5. Impact	If the asset is lost or compromised, how would it affect budgets, compliance obligations, and core activities?
	Document the steps you have taken and the outcomes.

Protect: Your essential security layers

Every education institution needs a set of essential security components—a mixture of documented policies, databases, hardware, network security solutions and endpoint protection.

Regulation		
Internet use policy		Asset management
Network		
Email security	Next-gen firewall	Backup solution
Endpoints		

The award-winning ThreatDown Education bundle delivers 10 layers of protection and safeguards Windows PCs, Chromebooks, Macs, and mobile devices.

Vulnerability assessment	Identify and prioritize weaknesses in your environment.
Patch management	Automated app and operating system updates.
Incident response	Automated endpoint remediation.
Next-gen AV	Best in class threat monitoring and isolation.
EDR	Award-winning Endpoint Detection and Response.
Device control	Prevent infection from peripherals.
Application block	Block unwanted applications.
Managed Threat Hunting	Identify and prioritize critical alerts 24/7.
Chromebook protection	Protect Chromebooks and Android mobile devices.
Ransomware rollback	Restore encrypted files up to 7 days after an attack.

Recover: A 10-step breach recovery plan

An institution's attack surface is constantly evolving as new individuals, devices, software, and data are introduced into the environment—and as cybercriminals adapt their tactics. Regardless of the number of protective measures in place, it is critical to remain prepared for the possibility of a security breach.

In the event of a breach, the following actions are recommended, in order:

1. Contain the attack	Isolate infected systems or networks to limit the impact of the attack.
2. Preserve evidence	In a serious attack you may be asked to preserve evidence for law enforcement, if you can.
3. Rollback if you can	Use ransomware rollback to restore systems to a known good state, if your solution allows.
	If you can't roll back
4. Understand the scope	Identify affected systems and data and prioritize critical systems for recovery.
5. Inform stakeholders	Inform senior leadership, PR, legal, cyber-insurance providers, security vendors and other stakeholders.
6. Seek assistance	Decide if you need expert assistance from law enforcement, vendors or other third parties.
7. Understand the breach	Identify compromised systems and accounts, and any persistence mechanisms left by attackers.
8. Rebuild	Use known good system images and backups to restore critical systems.
9. Reset, patch, upgrade	Reset passwords, patch vulnerable software, and implement missing security measures.
10. Learn what you can	Use what you have learned from the attack to improve your protection and policies.

Breaches can be extremely stressful. The individuals handling the incident should prioritize their actions, communicate clearly, take care of each other, and be encouraged to ask for help.

Learn more

The ThreatDown bundle for education is tailored for the needs of schools, colleges, school districts, and service providers working in the education sector.

The bundle simplifies staff and student device protection with layers of award-winning protection:

- Attack surface reduction, next-gen AV, and Endpoint Detection & Response.
- Mobile security that unifies protection across Chromebook, iOS, and Android devices.
- 24x7x365 managed detection and response service.

And it delivers ease of use to minimize management effort and optimize performance:

- Single, cloud-based console for deployment, configuration, management, and reporting.
- Single, lightweight agent for the entire endpoint security stack.

Get started today >