Cybersecurity for K-12 Schools and Districts

Implementing data security procedures for a school or district should be a dynamic and ever-evolving process. Incorporating powerful hardware solutions, strategic infrastructure countermeasures and—above all—comprehensive faculty training are just some of the cybersecurity actions school leaders must take to deal with this insidious and highly-sophisticated assault against sensitive school data.

According to a report published by security firm Armor, more than 500 schools were hit with ransomware within the first nine months of 2019. A similar report from antivirus maker Emsisoft claims to have identified 62 incidents affecting 1,051 schools and colleges. The report also goes on to say that attacks through managed service providers (MSPs) are on the rise, with email and attachments continuing to be the attack vectors of choice. Two Long Island, New York school districts, for example, were hacked and forced to pay $88,000 in ransom in the summer of 2019.

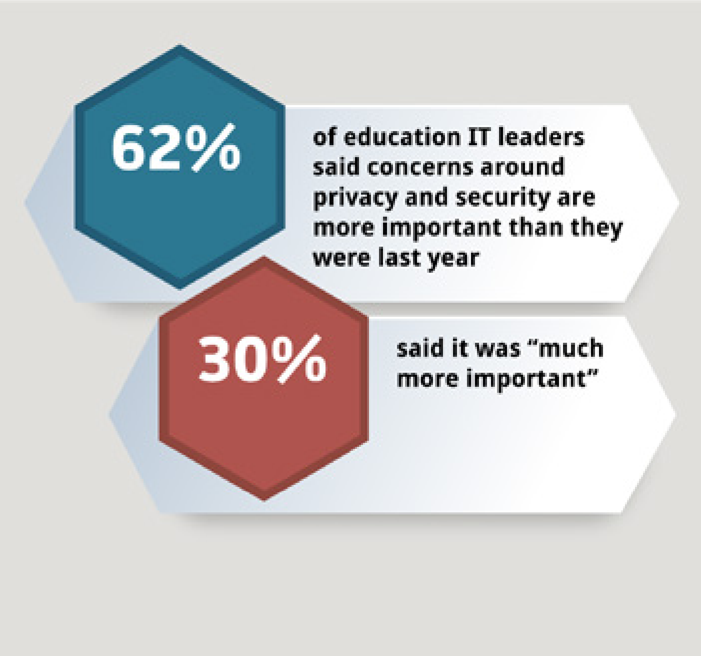
Hackers typically infiltrate a school server by sending a phishing email to an administrator or administrative assistant. This person will often inadvertently click on the email and—when they leave school—the illicit program activates and downloads on to the school server and will often change passwords and lock the school out of their own data.

Follow the Leadership

The CoSN 2017 IT Leadership Survey reports that 62% of education IT leaders said concerns around privacy and security are more important than they were in the year previously, with 30% saying it was "much more important". Cybersecurity ranked as their third highest priority with privacy fourth, up from 2014 where privacy was ranked second to last.

Legislators and lawmakers are trying to address the issue of data breaches in educational data. According to the Data Quality Campaign, 36 states introduced 95 bills and passed 31 new laws in 2017 that addressed the collection, linking, and subsequent governance of education data. Additionally, legislators in 42 states introduced 183 bills and passed 53 new laws that explicitly addressed how their state collects, manages, uses, reports, and protects data about students and schools.

All of these laws are in some way a derivative of the General Data Protection Regulation (GDPR): the most comprehensive data protection and privacy regulations. Originating from the United Kingdom, the GDPR makes it the responsibility of a company or organization to protect any data that it collects. This means that a citizen in the European Union can sue a company that has their data in the event of a breach.



Regulations Overview

GDPR: General Data Protection Regulation
A regulation in European Union (EU) law on data protection and privacy in the EU and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas.

FERPA: Family Educational Rights and Privacy Act
Passed by Congress in 1974, the act grants four specific rights to the student. These rights begin as soon as the student enrolls or registers with an academic program of the university.

COPPA: The Children's Online Privacy Protection Act
A law created to protect the privacy of children under 13. The Act was passed by the U.S. Congress in 1998 and took effect in April 2000. COPPA is managed by the Federal Trade Commission (FTC).

CIPA: Children's Internet Protection Act
Enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program.

PPRA: Protection of Pupil Rights Amendment
A federal law that affords certain rights to parents of minor students with regard to surveys that ask questions of a personal nature.

CCPA: California Consumer Privacy Act
A new consumer privacy law that went into effect on January 1, 2020. CCPA is a state statute intended to enhance privacy rights and consumer protection for residents of California.

To Avert, You Must First Understand

Schools and districts must design networks with both privacy (informed consent and owning up to breaches) and security (avoiding breaches as much as possible) in mind, utilizing specific threat personas.

First, there is the hacker that typically attacks from outside of the US (mostly Russia, China, and North Korea), looking for easy targets to exploit. Their most popular weapons are an email attachment virus that encrypts a school's database. Staff training on cybersecurity practices and a secure architecture that prevents intrusions from external parties are the best defense.

Then there are threats posed by people such as programming students who poke around looking for ways to change their grades, for example, or individuals who prey on assistants and secretaries who keep passwords on sticky notes. Some common architecture weaknesses in this scenario include Broken Authentication and Session Management, Security Misconfiguration and failure to restrict URL access. Staff training and measures such as roles and permissions to lock down access to only what's needed, login expirations, password managers, and data confidentiality agreements are also important so that faculty avoid accidentally being exploited for information.

Potential threats also include employees who accidentally leave sensitive reports and documents on printers or out in the open, and interns who utilize file-sharing apps such as Dropbox and Google Drive that put sensitive data at risk. Potential security measures include identity management, using de-identified data, data governance, security incident response protocols, and training on specific processes concerning risk.

Digging deep into these "bad actors" and their modes as well as their motives is the best way to thwart future attacks. Ask yourself and your school tough questions today to avoid having to explain your network's weaknesses tomorrow.

Learn more

Learn more about data privacy for K-12 education at CDW.