With 1,000+ schools cyberattacked in last 5 years, what can your district do to avoid being next?

By the New York State Association of School Attorneys

Schools in western New York were temporarily closed this winter due to cyberattacks. In-person classes were canceled in the Victor Central School District after malware locked users out of key systems (e.g., SchoolTool, Transfinder) in January. Both in-person and remote classes were halted in Buffalo Public Schools after a cyberattack in March.

The problem is widespread and getting worse. Since 2016, there have been 1,180 publicly disclosed cybersecurity-related incidents involving U.S. public schools, according to the K-12 Cybersecurity Resource Center. In August and September, 57% of ransomware incidents reported to federal authorities involved K-12 schools, compared to 28% of all reported ransomware incidents from January through July, according to the Cybersecurity & Infrastructure Security Agency, which is part of the federal government.

Unfortunately, the question is not "if" your school district will become the victim of a cyberattack, but when. If successful, the consequences often include disruption of critical school operations, exposure of sensitive personally identifiable information (PII) of students, teachers or staff, and, in many cases, ransom demands.

The U.S. Treasury Department has noted that cybercriminals are getting more sophisticated [see sidebar]. Every school board in New York State should be asking questions about the adequacy of the district's defenses for a potential cyberattack and ensure that appropriate policies (including insurance policies) are in place. This article will explain the most common threats and make recommendations for action consistent with state and federal law.

Types of cyberattacks

Cyberattacks come in many forms. They include:

Phishing. More than 90% of cyberattacks involve receipt of seemingly legitimate emails that invite users to reveal personal information or click on links that ultimately install malicious software. For example, employees may receive an email from the "Head of School" asking them to submit personal information for W-2 forms, but examination of the sender's email address will reveal it to be a fake. Thus, school staff should be trained periodically on how to detect phishing emails and websites, as well as how and to whom phishing emails should be reported.

Ransomware. After malicious software encrypts data, the target school district may be contacted and offered a key if a ransom is paid (often via bitcoin, which is untraceable). The FBI estimates that paying a ransom could cost between $100,000 and $300,000, but could be negotiable. For instance, a school district on Long Island paid hackers nearly $100,000 in 2019 to recover data from a ransomware attack. That same year, the Syracuse City School District decided to pay a $50,000 insurance deductible to restore its computer system because of a ransomware attack, according to news reports. Best practice dictates that school districts have reliable backup servers that are not accessible by the rest of the district's network and are regularly backed up.

Distributed denial-of-service. A computer system can be overwhelmed by multiple, simultaneous requests called a distributed denial-of-service (DDoS) attack. These are not preventable in a system that permits remote access. Thus, it is critical to monitor a school's network to detect DDoS threats early on and develop a policy or procedure to respond to such an attack. Additionally, school districts may consider obtaining cloud services to mitigate DDoS attacks by focusing on protecting the underlying internet connection or higher-level web servers.

Data breaches. Data breaches occur when secure confidential information is released to an insecure environment. Data are then either copied, transmitted, viewed, stolen, or used in an unauthorized manner. In the education sector, while 81% of data breaches are caused by external attackers, the remaining 19% are caused by a combination of accidental, negligent, and intentional harmful activity by insiders, according to the National Association of Independent Schools. Data loss prevention solutions detect and prevent data breaches but these, like cloud services, can be cost-prohibitive. So, school districts may consider other cost-effective cybersecurity measures, including encryption services, staff training, obtaining insurance coverage to ease the cost of damage, and/or a third party audit of school technology systems.

Liability issues

When cyberattacks or data breaches occur that compromise student data and/or teacher or principal data, school districts have specific obligations under state and federal law. The federal Family Education Rights and Privacy Act (FERPA) and New York State Education Law Section 2-d and corresponding regulations (Part 121), require school districts to report and guard against unauthorized acquisition, access, use or disclosure of student data and/or teacher or principal annual professional performance review (APPR) data by or to a person who is not authorized to acquire, access, use or receive it.

Noncompliance with data privacy statutes and regulations may expose schools to significant liability, including monetary fines and/or legal action. For instance, students in the Miami-Dade school district sued the school board in 2017 after their social security numbers were inadvertently posted online. In that case, the students requested monetary damages and an "overhaul" of school district policies on the protection of student information. They also filed a complaint with the U.S. Department of Education for a violation of FERPA.

Proactive measures and steps forward

School officials should consult with their insurance carriers to discuss coverage and/or protection as it relates to cyberattacks, including demands for ransom payments. If they have not already done so, school boards should adopt policies relative to data protection and security including appropriate breach response and notification procedures. They should ensure that there is a chain of command and protocol to follow in response to a cyberattack.

[Editor's Note: Contact NYSSBA Policy Services for sample policy and regulation No. 8635, Information and Data Privacy, Security, Breach and Notification. See also "Switch to online learning highlighted obligation to protect student data" in the June 8, 2020 issue of On Board.]

Contracts with all third-party vendors that have access to or receive student or teacher or principal data from the school must be in accordance with Education Law Section 2-d to ensure that data is protected both during and after the term of contract. (Your school attorney can assist in such matters.)

State Regional Information Centers provide many services involving district computing and protection of data, and they can provide recommendations for employees to avoid falling for phishing emails. In addition, school districts should consider conducting an audit to assess their electronic or cyberspace vulnerabilities. For instance, schools should examine whether those employees who have access to personal or sensitive information, such as social security numbers, actually need that information in order to perform their jobs.

Backups are essential but not foolproof. Third-party cybersecurity companies may provide guidance and troubleshoot with school districts as to how to safeguard their data.

Should an incident occur, school officials should work to identify who was impacted and who or what caused it, shut down all systems and disable the network, identify how the technology was impacted, host an after-action review or lessons learned meeting, including a discussion as to whether or how existing policies or plans should be revised or revisited.

Preventing cyberattacks can be costly, complex and time-consuming. School board leadership and administrative preparedness can make the difference between your school district suffering a paralyzing cyberattack and experiencing a nonevent.

Freedman

Menasco

Members of the New York State Association of School Attorneys represent school boards and school districts. This article was written by Andrew Freedman and Lindsay Menasco of Hodgson Russ LLP.

'Increasing sophistication' of cybercriminals documented by U.S. Treasury Department

By Eric D. Randall
EDITOR-IN-CHIEF

In an advisory issued in October, the U.S. Treasury Department noted "increasing sophistication of ransomware operations" and a pattern of larger financial demands nicknamed "big game hunting."

Threats include:

Fileless ransomware. "Fileless ransomware is a more sophisticated tool that can be challenging to detect because the malicious code is written into the computer's memory rather than into a file on a hard drive," according the Treasury Department's Financial Crimes Enforcement Network (FinCEN). This method "allows attackers to circumvent off-the-shelf antivirus and malware defenses."

Networks of cybercriminals. "Some ransomware groups are … forming partnerships to share advice, code, trends, techniques, and illegally-obtained information over shared platforms," according to FinCEN. This includes free sharing of malicious codes and tools.

Double extortion schemes. Double extortion involves "removing sensitive data from the targeted networks and encrypting the system files," according to FinCEN. "The criminals then threaten to publish or sell the stolen data if the victim fails to pay the ransom."

Read the Treasury Department advisory at bit.ly/39ifcmD. Also, the federal Cybersecurity & Infrastructure Security Agency has K-12 security guides at bit.ly/3fznc6S.