Controlling Spiraling Cyberattacks

Understanding today's cyber landscape is essential for all school leaders.

By Joseph Saracino

ANATOLIR/STOCK.ADOBE.COM

Cybercriminals have increasingly made schools a primary target. The K–12 Security Information Exchange, a Virginia-based nonprofit providing cybersecurity services to schools, reported having tracked over 1,200 cyberattacks on U.S. public school districts since 2016, including 209 ransomware attacks, 53 denial-of-service attacks, 156 Zoom-bombing attacks, and 110 phishing attacks. Primary and secondary schools, public and private schools, and colleges and universities have all been victims of cyberattacks.

In its report titled *The State of K–12 Cybersecurity: 2020 Year in Review*, the K–12 Cybersecurity Resource Center refers to 2020 as a record-breaking year for cyberattacks on schools. It reports that 408 publicly disclosed cyberattacks against K–12 schools or districts occurred in 2020, an increase of 18% over the prior year.

As it compiles data for 2021, the organization anticipates a higher number of incidences; data from other sources support this expectation. In July 2021, Check Point Software noted a 29% increase in cybercriminals' targeting schools worldwide over the previous six months.

As the data suggest, it is no longer a matter of if, but when your school may become the next target of ransomware, phishing, denial of service, or other cyberattacks. Understanding today's cyber landscape related to the education market is essential for all school leaders. Knowing what best practices should be deployed is critical.

Latest Developments in School Cyberattacks

Schools are under siege by cybercriminals looking to access valuable, sensitive data, such as the addresses, phone numbers, and financial information of students or their parents, as well as that of educators. A high percentage of cyberattacks on schools stems directly from their information technology (IT) vendors. K–12 Security Information Exchange data found that 75% of all K–12 school breaches in 2020 were implemented through the schools' vendors. These and other attacks were already increasing before the pandemic, but remote learning and the technology vulnerabilities it introduced gave cyberthieves more ammunition to fuel their attacks.

In fact, having access to more technology in education is generally regarded as a good thing; however, it opens up a school to more cyber land mines and gives cyberthieves new pathways for ransomware and malware attacks, and others.

> **No geographic region is off-limits for school cyberattacks; however, some areas have been dubbed "hot spots."**

No geographic region is off-limits for school cyberattacks; however, some areas have been dubbed "hot spots." These targets are states with the most significant number of institutions and largest student bodies, such as California, Illinois, New York, Ohio, and Texas.

Following are some of the recent high-profile cyberattacks on schools:

- The January 4, 2022, ransomware attack on Finalsite, a leading school website services provider, disrupted access to its network of 8,000 schools and colleges in an estimated 115 countries.
- The January 2022 cyberattack on Albuquerque Public Schools forced the cancellation of classes for approximately 75,000 students for two school days.
- In a business email compromise attack on the San Felipe Del Rio Consolidated Independent School District, the district's comptroller was sent phishing emails from cyberthieves pretending to be officials from the financial institution to which the district makes bond payments. As a result of the attack, three of the district's four bond payments were diverted to the cybercriminals' financial account; the district sustained a loss of $2 million.
- Classes were disrupted for school systems in Baltimore County, Maryland, and Miami-Dade County, Florida, as well as in New Jersey and Wisconsin school districts, among others.

Many more cited examples of attacks have prompted a heightened response by school leaders.

Education Leaders' Responses

Reports of cyberattacks have become an eyeopener for school leaders who recognize the need to prioritize cybersecurity and formalize their related practices. After the Finalsite breach, for example, many school leaders realized they needed a tighter communications policy between themselves and their vendors in the event a vendor experiences a cyberattack that affects the schools. Further, many school systems now require their vendors to submit a cyberattack response plan for alerting the schools regarding attacks, along with measures to be implemented to restore their systems' secure operations.

Schools are instituting other policies, including allowing only school devices to access the network, providing access to secure data on a need-to-know basis, and eliminating guest networks. Educating all constituents, including vendors, faculty, parents, and students, regarding sound cyber practices has also become a priority for many schools.

That education covers such practices as changing passwords regularly, ensuring that devices are protected with security software, and not opening suspicious emails. These and other essential measures should be adopted and incorporated into a comprehensive, proactive school cybersecurity program.

Measures to Manage and Mitigate Cyberattacks

In its October 2021 report to congressional requesters, *Critical Infrastructure Protection: Education Should Take Additional Steps to Help Protect K–12 Schools from Cyber Threats*, the Government Accountability Office (GAO) laid out federal resources for K–12 schools. Of note was a data breach scenario training kit, a guide for ransomware prevention and response, a notice on the use of malicious emails to compromise operations, a distributed denial-of-service alert, and a document covering videoconferencing disruptions.

The report's publication came close to President Biden's October 8, 2021, signing of the K–12 Cybersecurity Act of 2021, which authorized the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) to study cyber risks affecting K–12 schools and to provide recommendations for enhanced cybersecurity.

In its report, the GAO presented an overview of the cyber landscape affecting schools. It identified the players in cyberattacks (i.e., criminal groups, terrorists, nations, and insiders with access to a school's information system and enterprise). It delineated the responsibilities and roles of CISA, the Department of Education's Office of Safe and Secure Schools (OSSS), and the Federal Bureau of Investigation.

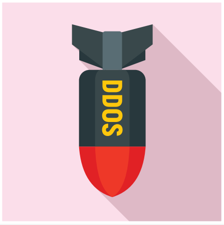
THE MOST COMMON FORMS OF CYBERATTACKS

Malware is malicious software that is placed on computers or a network and enables the cybercriminal to take control of the computer to monitor the user's keystrokes and actions and access confidential data. The malware gets into a computer when the user clicks on a link or opens an attachment.

SQL (structured query language) injection attacks target servers that store proprietary/critical data and use SQL to manage their databases. An SQL injection attack uses malicious code to target the server and cause it to convey privileged information.

Ransomware attacks by hackers deploy malicious software to encrypt a school district's data and demand a ransom in return for the district's regaining access to its data.

Phishing attacks occur when a cybercriminal sends emails, presumably from a legitimate organization (often one with which the individual or organization has a relationship), requesting personal data (e.g., financial account information, passwords, etc.)



Denial-of-service attacks temporarily shut down a machine or network and render it inaccessible to its intended users.

ANATOLIR/STOCK.ADOBE.COM

In addition, the report presented the programs and services the entities developed to help K–12 schools incorporate cybersecurity measures. It is important to know, however, that the report states that the OSSS has not kept the education subsector's cybersecurity plan up-to-date, admitting that it was last published in 2010, although it was required to update the plan every three years. As a result, the plan no longer reflects the current cyber environment.

Key Initiatives

What is clear from the report and the increasing cyberattacks on the education sector is that schools must be proactive in their own organization's cybersecurity. That requires several key initiatives:

Detection. Every school should begin by benchmarking its current cybersecurity status. To ensure its integrity, benchmarking should be performed by a third-party cybersecurity firm and not the school's internal IT department or its managed services provider.

Detection involves two components: (1) a comprehensive vulnerability assessment to evaluate the school's IT systems and assess risk levels and (2) penetration testing, also known as "ethical hacking," to determine how easily cybercriminals could enter the school's IT systems, including the network, ports, database, emails.

Mitigation. Following the vulnerability assessment and penetration testing, measures should be taken to mitigate system weaknesses and vulnerabilities. Such measures range from installing firewalls, encryption software, and end-point protection to multifactor authentication, password and SSH (secure shell protocol) key management, and solutions to lock access to proprietary data.

Best practices. Best practices include data backups and backup data recovery, along with keeping up with software updates and limiting access to sensitive data to authorized staff members.

Cybersecurity policies. Policies—including best practices, responses to cyberattacks, and related communications—should be formalized in a cybersecurity policy manual and provided to all vendors and staff members who manage, use, or have access to school information systems and technology.

Training. Cybersecurity awareness training for staff should be conducted regularly to ensure that cybersecurity policies are understood and adhered to, and that staff are kept abreast of the latest developments in cyberattacks on schools. As part of this training, staff should be educated regarding the various forms of cyberattacks, including the most common forms, highlighted in the sidebar on the previous page.

> **Vigilance is essential for avoiding financial and reputational damages stemming from a lax attitude toward cyberattacks.**

A cyber incident management and reporting plan. This comprehensive plan helps the organization prepare for, detect, respond to, and recover from network security incidents.

Regular review of cyber insurance coverage. A regular review ensures that the insurance covers the latest threats and is adequate in covering the school's total exposures and liabilities.

Closing Thoughts

Avoiding the many land mines dotting today's cyber landscape is not easy. It requires heightened awareness and the commitment of education leaders and their staffs to follow prudent cybersecurity practices.

Comparitech, a security testing site, estimates that 77 ransomware attacks on 1,740 schools and colleges took place in 2020, affecting over 1.36 million students and costing the schools approximately $6.62 billion in downtime alone. Not included were the costs associated with recovering data, restoring the computers, and implementing new security measures. These data reflect just one type of cyberattack and not the countless others that have affected schools. Vigilance is essential for avoiding financial and reputational damages stemming from a lax attitude toward cyberattacks.

Joseph Saracino is president and CEO of Cino Security Solutions, LLC, in Coram, New York. Email: jsaracino@cinoltd.com

This article originally appeared in the May 2022 School Business Affairs magazine and is reprinted with permission of the Association of School Business Officials International (ASBO). The text herein does not necessarily represent the views or policies of ASBO International, and use of this imprint does not imply any endorsement or recognition by ASBO International and its officers or affiliates.