“Our Biggest Nightmare Is Here”

Cyberattacks are targeting school districts. How can schools respond to keep data and systems secure?

DREAMSTIME / PHOTO ILLUSTRATION *EDUCATION NEXT*

ON THE NIGHT OF SEPTEMBER 2, 2019, Assistant Superintendent for Compliance and Information Systems Bhargav Vyas received a system-failure warning for Monroe-Woodbury Central School District in Central Valley, New York. With his team, he chose to shut down the district's entire computer network. Then, at 7:30 the next morning, he got a call from one of his leading techs, who was bringing the domain controllers back up after the previous night's shutdown.

"Our biggest nightmare is here," the tech said.

That was when Vyas knew a cybersecurity attack was happening.

* * *

Of the 17 industries studied by information-security company SecurityScorecard, the education sector ranked as the least secure in 2018, with the highest vulnerabilities present in application security, endpoint security, and keeping software up to date. Online learning, which has increased gradually over the past decade and significantly since March 2020, has only exacerbated the possibility of exposing staff and student data to unauthorized parties. The 2020 calendar year saw a record-breaking number of publicly disclosed school cybersecurity incidents—a grand total of 408 across 377 school districts in 40 states, according to the K–12 Cybersecurity Center. This represents an 18 percent increase over the 2019 calendar year total and a rate of more than two incidents per school day throughout 2020. These cyberattacks impacted taxpayers, district staff, and students, leading to school closures, millions of dollars stolen, and data breaches linked to identity theft and credit-card fraud.

Though these attacks affected only a small fraction of the overall number of schools and districts in the U.S., the frequency may increase as more lucrative targets, like corporations and banks, mount a better defense. According to the Consortium for School Networking's 2019 K–12 IT Leadership Survey Report, rather "than focusing on corporate targets, which are devoting increased resources to cyber defenses," hackers are turning to "more vulnerable sectors such as school districts, universities, and nonprofits."

School districts' networks are the perfect target for cybercriminals because they house a large amount of personal data but exist in a milieu not necessarily attuned to the threat of attack. While hackers' individual motivations run the gamut, most of the attacks on school districts have been tied to cybercriminals looking for low-risk, high-return financial payoffs—which embattled district decisionmakers are willing to provide if it means keeping student and staff information private.

How Cyberattacks Happen: Phishing and Distributed Denial-of-Service Attacks

According to the Consortium for School Networking, more than 90 percent of cyberattacks in schools start with phishing campaigns, which include "spear phishing" and business-email compromise attacks. Spear phishing is characterized by a focus on specific individuals or groups within a larger organization; these attacks usually get a user to reveal personal

By EILEEN BELASTOCK

information or install malicious software, or malware, on their computer. In a business-email compromise attack, cybercriminals impersonate a trusted party, usually a senior executive, to obtain payments or financial information. In a school-district context, business-email compromise is sometimes known as "Superintendent Fraud."

Phishing attacks have become more sophisticated and difficult to detect. During the 2019–2020 school year, the San Felipe Del Rio Consolidated Independent School District was hit by a business-email compromise attack. A news release from the U.S. Attorney's Office in the Western District of Texas explained how the attack worked: The school district's comptroller received phishing emails from cybercriminals posing as officials at the financial institution to which the district makes bond payments. Three of those bond payments were then diverted to the swindlers' financial account, which cost the district more than $2 million, according to the release.

Bhargav Vyas, assistant superintendent of Monroe-Woodbury Central School District in New York state

Schools and districts can also fall victim to distributed denial-of-service attacks, as the *Boston Globe* reported Boston-area districts Mansfield, Medfield, and Norton did during the 2020–2021 school year. In this type of attack, a targeted flood of internet traffic disrupts network availability by overwhelming the system and surrounding infrastructure. As a result, users are prevented from accessing payroll platforms, student schedules, and email applications, all of which are necessary to conduct the day-to-day operations of the school.

This disruption can be just as beneficial for cybercriminals as it is for students, who may want classes cancelled or a break from remote learning. In September 2020, a series of DDoS attacks targeting the Miami-Dade County Public Schools were traced to the IP address of a 16-year-old student at South Miami Senior High School, according to a news release from the school district.

In addition to the complete paralysis of a school system, most criminal DDoS attacks have a second purpose: to breach data and expose confidential or protected information that can be viewed, shared, and used as ransom.

Ransomware

While school networks are offline during a DDoS attack, hackers use malicious software to encrypt districts' data. Districts are then forced to pay hackers a ransom to regain access to their data—hence the term "ransomware." As of August 2021, ransomware attacks have disrupted 58 education organizations and school districts in the U.S., including 830 individual schools, according to *Politico.* These attacks sometimes have devastating consequences: In March 2021, the *Miami Herald* reported that Broward County Public Schools could not pay a $40 million ransom, and 26,000 stolen files, which included student and staff Social Security numbers, addresses, and birthdates, were published online.

Of the 17 industries studied by information-security company SecurityScorecard, the education sector ranked as the least secure.

Most school districts lack strong security protocols because they have small IT teams and significant budgetary constraints, so it may seem from the outside that education organizations are not making cybersecurity a priority. This assessment, however, does not reflect the progress being made in districts across the country.

Thwarted Ransomware Attacks: Case Studies

Monroe-Woodbury Central School District

Back to Monroe-Woodbury Central School District. As soon as the IT team knew an attack was underway, they notified Superintendent Elise Rodriguez and the other assistant superintendents. Rodriguez informed the board of education, and then the public relations director and communications team contacted the business office, the district attorney, and the insurance company. Within an hour, the district had an incident response team working with Vyas to contain the attack, assess the damage, and develop a mitigation plan. The cybercriminals had just started targeting the district's servers when the storage area network shut down, so, luckily, they had nowhere to go to do more damage.

Superintendent of Monroe-Woodbury Central School District Elise Rodriguez

Once the team determined that they had stopped the ransomware, the district focused on restoring weeks' and months' worth of data from offline and cloud-based backup systems. It took the district a couple of days to build up a Microsoft infrastructure, but by the end of the first week, 70 percent of mobile devices were up and running. At the end of the second week, all systems were up and running, and Wi-Fi was brought back online

for 3,000 student and staff devices and computers.

Vyas reflected that it "was strategic on our part—not from the ransomware perspective, but a resources perspective—that we had an updated disaster recovery plan that identified the location of our data in all systems, as well as a robust redundancy system. This strategic move mitigated any further damage and communication."

Prior to the attack, the district had also gotten an assessment of their network from the National Institute of Science and Technology. In January and March 2019, the IT team used the audit recommendations to "plug the holes," which, in hindsight, could have been a factor in mitigating the effects of the cyberattack.

The IT team tried to learn from the attack. Though they had no proof, they believed that allowing personal devices to connect to the school network may have been a factor in the attack. The district therefore changed its policies: Only school devices were allowed to access the network, and guest networks were eliminated.

Rodriguez established scenario-based cybersecurity training, because "security is not just a technology concern; it's a district concern." Vyas continues to educate the school community, including the school board, about the latest trends in cybersecurity because, as he puts it, "people forget."

Haverhill Public Schools

The attack on Haverhill Public Schools in Haverhill, Massachusetts, started shortly after midnight on Wednesday, April 7, 2021. By 2:30 in the morning, Director of Technology Doug Russell and Systems/ Network Engineer Don Preston had been alerted of system failures. They realized that this was more than just a standard system alert, and the team immediately shut down the network that connected all 15 district schools.

As soon as Russell and his team understood the extent of the attack, they notified Superintendent Margaret Marotta. Marotta then informed the Haverhill Public Schools School Committee and other critical stakeholders. She became the central communications person, thus enabling the IT team to focus on mitigating the problem. Within a few hours, the district had implemented its crisis-recovery plan and connected with its IT consulting company, which joined with local police, state police, the FBI, the Department of Homeland Security, and the Multi-State Information Sharing and Analysis Center, an organization that helps local, state, and tribal governments with cybersecurity-incident response and remediation, to assess the situation. After a few hours of evaluating the network, the Haverhill team determined that 140 of the 13,000 district endpoint devices had been infected with the ransomware. Much of the virus had been funneled into the districts' virtual server environment, and most of those virtual servers had then detected the infection and shut down—exactly as they had been designed to do.

Authentication and rostering servers were up and running by six o'clock in the evening on the day of the attack. Five days after the incident, the internet had been restored in all 15 buildings, with 98 percent of the systems fully functioning. The email system took two and half weeks longer to be fully restored.

DREAMSTIME

"One of the things that saved us was the transition to laptops for staff during the pandemic," said Doug Russell of Haverhill Public Schools.

"One of the things that saved us was the transition to laptops for staff during the pandemic," Russell said. Most staff members' computers were not on the district network when the attack happened.

Russell added that another helpful mitigating factor was "a change that we made a couple of years ago" to "our whole virtual environment," which meant there was no clear path for the ransomware to follow. Also, the cyberattack did not impact district financial records because the payroll system was hosted by the City of Haverhill on a completely different network. Finally, Russell explained that moving many systems to cloud hosting made the attack less severe than it would have been if the district had hosted all of those systems internally.

The Multi-State Information Sharing and Analysis Center's investigation of the attack is ongoing, and the district has yet to confirm if any personal data was compromised. The team at Haverhill Public Schools did learn that they needed to upgrade existing systems and backup options, though. Before the attack, they had data snapshots, and the district operated with two different systems running at the same time. "So even though everything was still being snapshot and backed up, we realized that some of those systems, if they were to shut down, or if they would have been infected the wrong way, wouldn't have gotten the last couple snapshots that we needed to recover," Russell said.

The 2020 calendar year saw a record-breaking number of publicly disclosed school cybersecurity incidents—a grand total of 408 across 377 schools districts in 40 states, according to the K–12 Cybersecurity Center.

Working with an IT consultant and the district crisis response team, as well as Marotta's support and additional funding from the Haverhill School Committee, Russell and his team determined the need to increase redundancy and upgrade their anti-malware software and anti-ransomware software.

"I feel like if that would have been running, or something would have been running better, it probably would have stopped it even sooner, and we would have had fewer servers to restore," reflected Russell.

Moving systems to cloud storage might mitigate some of a cyberattack's effects, as it did for Haverhill Public Schools.

What Can Districts Do?

Cybersecurity training

According to the October 2020 IBM Education Ransomware Study, which involved interviews with 1,000 educators and 200 administrators, administrators were "20 percent more likely to receive cybersecurity training than educators" though they were "still unaware of critical information relevant to protecting their schools." Eighty-three percent of administrators expressed confidence in their school's ability to handle a cyberattack, for example, but more than 60 percent of them did not know if their school had a mitigation plan.

About 90 percent of the time, cyberattacks happen due to human error, said Haverhill's Russell. The source of the Haverhill Public Schools attack was a phishing email, which allowed the hackers to access a virtual remote server. In the wake of the attack, the school community took action and recognized the need for more cybersecurity training and, specifically, for secure password protocols through standardized requirements, such as making sure passwords are a certain length or have special characters.

Back up, back up, back up

A robust backup system is the best protection against an attack, and the most effective backup systems are a) cloud-hosted or offline, b) not tied to a district's domain, and c) inaccessible from the district network. The Monroe-Woodbury and Haverhill districts have used secure backup systems with redundancy for years, so when their virtual servers were attacked, they were assured the recovery of their data. Russell added that "a backup is vital" and that "if districts are not backing up correctly, they will never be able to recover" from an attack.

Cybersecurity insurance

In 2020, the average cost of a data breach was $3.79 million for districts and other education organizations in the U.S., according to IBM's annual report on data-breach costs. When the Manor Independent School District, a small district in Texas, was compromised by a phishing scam in January 2020, CBS Austin reported that it cost the community $2.3 million.

Most insurance companies now offer cyber liability insurance to school districts, for an average of $1,600 a year, according to AdvisorSmith. Though the cost varies based on size and location, districts could end up saving millions by adding this insurance to their yearly operational budgets. In November 2019, when Port Neches-Groves Independent School District in Texas was hit by a ransomware attack, a cybersecurity insurance rider on their district policy covered the $35,000 ransom demand, reported KBMT news. The district ended up getting back access to their systems—at the relatively low cost of a $2,500 insurance deductible. Cybersecurity insurance often covers not just the cost of the ransom itself, but of IT experts to analyze the breach, a marketing firm to manage the district's response, and lawyers to advise the best next steps, as well lost revenue. The insurance also provides credit monitoring for the students and staff whose records were exposed by the breach.

WHITE HOUSE

President Biden signed the K–12 Cybersecurity Act of 2021, which authorizes the study of cyberattacks and will lead to guidelines, recommendations, and toolkits for districts.

Other best practices

Districts can reduce infections by filtering at the email gateway, maintaining updated antivirus and anti-malware software, and using a centrally managed antivirus solution. In addition, because some attacks are accidental, districts should apply the principle of data governance, or giving users access only to the data they need to do their jobs. It is also critical that districts maintain a robust asset-management system, retain and secure logs from network devices and local hosts, and baseline and analyze network activity to determine behavioral patterns. While districts may feel vulnerable and helpless in the wake of an attack, these proactive, rather than reactive, actions will determine the overall impact of a cybersecurity attack.

The Work of Many

Districts cannot fight off the hacker hordes alone. Though the ESSER fund provides billions of dollars to school districts for support in the wake of Covid-19, the money allocated to support broadband access, equipment purchases, and remote-learning infrastructure does not cover districts' cybersecurity needs, such as upgraded firewalls. In June 2021, Senators Mark R. Warner and Susan Collins wrote a letter to Education Secretary Miguel Cardona advising the department to make Covid-19 relief funds available for cybersecurity resources. The letter also recommends that the U.S. Department of Education engage with school districts to increase awareness of the need for more robust cybersecurity measures.

On October 8, 2021, President Biden signed the K–12 Cybersecurity Act of 2021. This bill authorizes the Cybersecurity and Infrastructure Security Agency to study the specific risks impacting K–12 institutions, develop recommendations for cybersecurity guidelines, and create an online toolkit districts can use for implementation. Additionally, a bipartisan group of four House members introduced the Enhancing K–12 Cybersecurity Act in June 2021. This law would direct the Cybersecurity and Infrastructure Security Agency to create a cybersecurity information exchange, a K–12 incident reporting registry, and a $10 million, annual technology-improvement program.Organizations such as the Consortium for School Networking, State Educational Technology Directors Association, and National Association of State Chief Information Officers supported the bill.

When it comes to a cyberattack on a school district, it is no longer a matter of if but when. No longer does the danger zone start at the perimeters of district infrastructure and network. The danger zone now lies within the walls of school districts themselves. We must assume that, whether they are malicious or accidental, bad actors exist within our own systems.

Eileen Belastock is director of technology and information at Nauset Public Schools in Massachusetts.