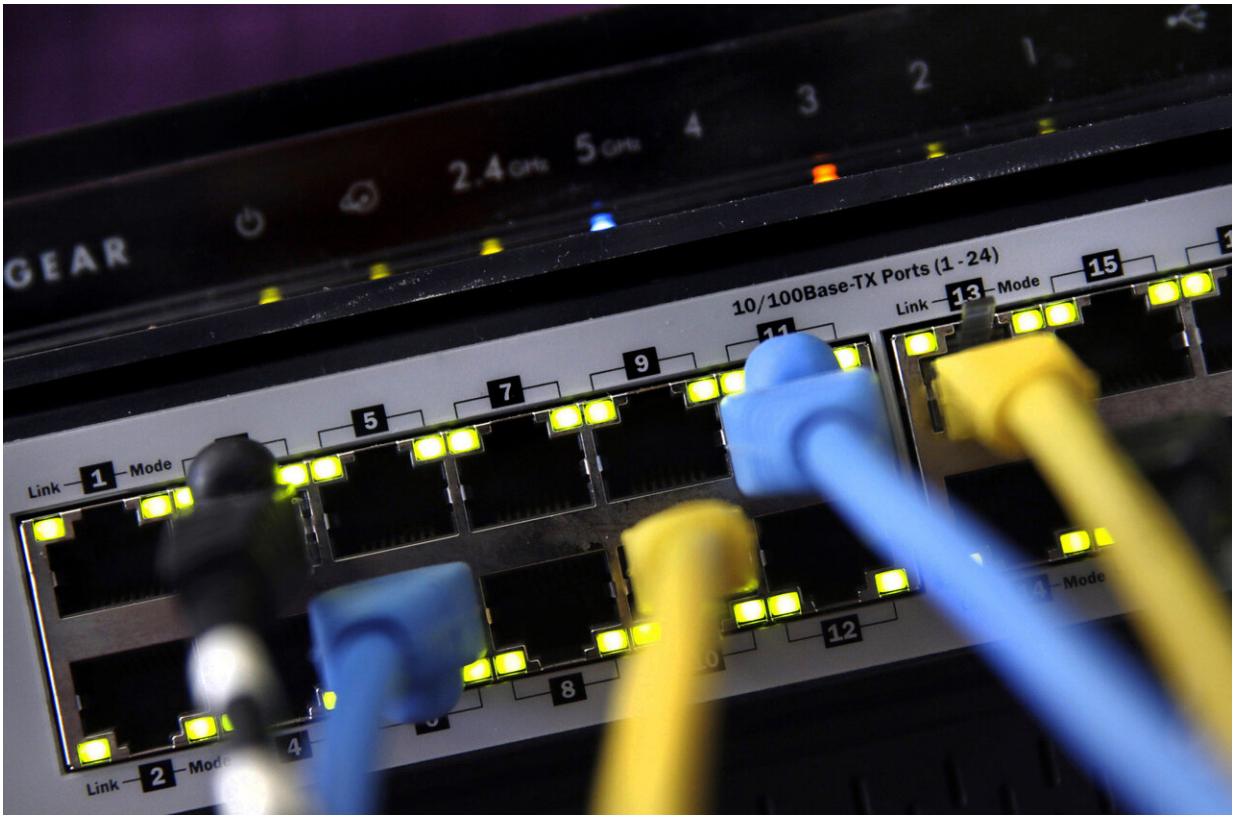
Cyberattacks inflict deep harm at technology-rich schools

July 16 2019, by Michael Melia



In this June 19, 2018, file photo, a router and internet switch are displayed in East Derry, N.H. The FBI said cyberattacks have become common at schools, which are attractive targets because they hold sensitive data and provide critical public services. Malicious use of the data could lead to bullying, tracking and identity theft, the agency said. (AP Photo/Charles Krupa, File)

Over six weeks, the vandals kept coming, knocking the school system's network offline several times a day.

There was no breach of sensitive data files, but the attacks in which somebody deliberately overwhelmed the Avon Public Schools system in Connecticut still proved costly. Classroom lesson plans built around access to the internet had come to a halt.

"The first time I called the FBI, their first question was, 'Well, what did it cost you?'" said Robert Vojtek, the district's technology director. "It's like, 'Well, we were down for three quarters of a day, we have 4,000 students, we have almost 500 adults, and teaching and learning stopped for an entire day.' So how do you put a price tag on that?"

The kind of attacks more commonly reserved for banks and other institutions holding sensitive data are increasingly targeting school systems around the country. The widespread adoption of education technology, which generates data that officials say can make schools more of a target for hackers, also worsens an attack's effects when instructional tools are rendered useless by internet outages.

Schools are attractive targets because they hold sensitive data and provide critical public services, according to the FBI, which said in a written statement that perpetrators include criminals motivated by profit, juvenile pranksters and possibly foreign governments. Attacks against schools have become common, the FBI said, but it is impossible to know how frequently they occur because many go unreported to law enforcement when data is not compromised.

Attacks often have forced districts to pull the plug on smart boards, student laptops and other internet-powered tools.

Schools in the Florida Keys took themselves offline for several days last

September after a district employee discovered a malware attack. Monroe County schools Superintendent Mark Porter said teachers had to do things differently but adapted quickly.

"I heard a little grumbling at the beginning and then the comment was, 'I guess we'll have to go old school,'" Porter said. "And they went back to work and did it the way they probably did it just a few years ago."

Schools with few or no employees dedicated to information security often are surprised to find themselves as targets.

The 2,000-student Coventry Local School District in Ohio had to close schools in May as staff worked to fight a virus of that had infected the network. The FBI helped to guide the district through the recovery and offered assistance on best practices.

The school system did not have cybersecurity insurance, said Kelly Kendrick, the district's technology director, and her three-person department is still working to debug devices affected by the attack.

FBI officials told the district that the attackers apparently did not obtain sensitive information, but that it was clear they were after data of some kind, she said.

This July 12, 2019, photo shows the board of education offices in Avon, Conn. A denial of a service cyberattack overwhelmed the Avon school district's technology systems in late 2017 and brought to a halt instruction built around access to the internet. The FBI said cyberattacks have become common at schools, which are attractive targets because they hold sensitive data and provide critical public services. Malicious use of the data could lead to bullying, tracking and identity theft, the agency said. (AP Photo/Michael Melia)

"Why this little school in Akron, Ohio? Why was it a target?" Kendrick said. "It has really opened my eyes to how data of any kind is marketable, sellable."

In September, the FBI issued a public service announcement warning the

growth of education technologies and widespread collection of student identification data along with other information including academic progress and classroom activities "could have privacy and safety implications if compromised or exploited."

Malicious use of the data could lead to bullying, tracking, identity theft and other threats, it said.

Penalties can be severe. Students suspected of involvement in disruptive cyber pranks often have been hit with felony charges.

And in March, Olukayode Lawal, a Nigerian man living in Smyrna, Georgia, was sentenced to 10 months in prison and ordered to be deported for his role in an email scheme that used tax information from Connecticut school employees to falsely claim tax refunds.

In many cases, school officials say they never learn who was behind the attacks.

In North Dakota, where a third of schools statewide were hit with a malware attack last year, it was traced to North Korea, although it's unclear if that country was the origin of the attack or just the location of a device that was used as a stepping stone, according to Sean Wiese, the state's chief information security officer.

School networks "may be considered easy targets because they're a little bit more open than your traditional corporate culture," Wiese said. "I do feel that is changing, just not quickly enough."

In New York state, U.S. Sen. Chuck Schumer called on the U.S. Department of Homeland Security last October to investigate and help prevent future intrusions after a series of attacks caused outages at 50 school districts.

The denial-of-service attacks, designed to overload and deny access to the network, he said, "subverted teacher lesson plans and interrupted student learning."

The outages were disruptive particularly because many of the state's schools have issued digital devices to each student, part of a transition to a model where students spend part of a school day working at their own speed, according to Pam Mazzaferro, director of the Central New York Regional Information Center.

Vojtek, whose department was tasked with responding to the denial-of-service attacks on Avon schools in late 2017, said it was difficult being the one to answer to educators for why the network was down.

"It was just tough to get a handle on it and people are not resilient when it comes to their teaching resources," he said. "So if those are gone, somebody needs to pay."