HACKED

School districts on guard against ransomware attacks

Over 100 cyberattacks on school districts were reported last year

Justin Murphy

Rochester Democrat and Chronicle USA TODAY NETWORK

Look at school districts from the perspective of a hacker.

Districts maintain reams of sensitive information about employees, students and families, all of it online and accessible to varying degrees to hundreds or thousands of employees — not all of whom were paying particularly close attention in this year’s mandatory cyber-security webinar. With annual budgets in the tens or hundreds of millions, their pockets are deep, at least in theory, for the purposes of paying ransom.

And they can’t very well afford not to retrieve their data.

“On the list of things that keep me up at night, it’s a high one,” said John Miller, director of technology, data and program evaluation at the Hilton Central School District.

“If you ask any tech-related person in the field, they’ll tell you the same thing. … None of us want this to happen to us.”

More than 100 American school districts reported cyberattacks in 2018, likely a significant under-count of an inherently sensitive event. At least three Rochester- area school districts have been targeted in the last few years.

More recently, the Syracuse City School District and Onondaga County Public Library were victims of a ransomware attack apparently originating in Eastern Europe. Ransomware is software that locks down part or all of a website until the owner pays ransom, usually in difficult-to-trace cyber-currency such as Bitcoin.

GETTY IMAGES **Kindergartners Inieris Santiago, front, Shuaib Hussein, rear left, and Bryan Miller, work on computers in 2018 during a rotating activity unit at School 8.** JAMIE GERMANO/ROCHESTER DEMOCRAT AND CHRONICLE FILE PHOTO

“I think ransomware is growing as an attack vector because it works and because people pay,” said Bill Stackpole, a professor of computing security at Rochester Institute of Technology. “The major issue at this point is that there’s not really a good defense

eight felony counts after breaking into the former superintendent’s suspended account and accessing security camera footage, academic records and attendance reports, among other things. “This has the makings of a Hollywood movie,” Gates Police Chief against it. It just takes one person to click something they shouldn't be clicking on."

That means an employee falling for a phishing attempt — clicking on an innocuous-looking attachment that unleashes a virus on the network to which their computer is connected.

For a school district, potential information targets include employees' bank account numbers or personnel records as well as the health, academic and disciplinary information of students. Other data could have to do with vendors, law enforcement connections or sensitive legal issues.

Some of those things — for instance, employees' Social Security numbers — are easy for blackhat hackers to sell online. Academic records don't have the same cash value but, Stackpole said, are "pivotable" for use in a social engineering attack.

For instance, he said, a hacker who knows that a certain student is struggling in math could impersonate her teacher in a phishing email. When the student clicks on an attachment she believes is a worksheet with extra practice on fractions, her computer becomes infected as well.

Local districts affected

The Syracuse hacking struck a nerve for New York districts, but particularly in the similarly situated Rochester City School District. Its chief technology officer, Annmarie Lehner, said cyber- security threats have been "increasing exponentially" for the last several years, with phishing attempts at the top of the list. Twice in the last several years, she said, hackers impersonating top-level administrators have sent emails to payroll clerks attempting to change their direct deposit bank account. Neither attempt worked, she said, in part because of increased training and additional levels of security.

In some ways, small school districts are the most tempting target, as they likely have fewer safeguards in place. The Holley Central School District, for instance, saw personal information on thousands of employees and contractors exposed in a breach in 2016. Two local districts have been infiltrated in the last year by their own students. In Honeoye Falls-Lima last October, students gained access to academic records by hacking the superintendent's account. In May, a 17-year-old boy at Gates Chili High School was arrested on Jim VanBrederode said then. "It's a high school junior sitting around with his school-issued tablet."

Representatives from Holley and Gates Chili declined to comment. Honeoye Falls-Lima did not respond to requests for comment, nor did Greece, the largest suburban school district in Monroe County, or the state Education Department.

If in doubt, click 'delete'

There are two main ways for a school district or other organization to play defense against ransomware and other cyberattacks: technical barriers and training.

The former include, at the high end, sophisticated software for which schools often lack the necessary expertise and budget. More common means include two-step verification to log into devices remotely, or flagging email that comes from external accounts.

Lehner, from RCSD, attends an annual conference for school technology officers and usually returns with some new trick to keep employees' computers safe.

"Every year I come back ... and everyone says, 'Oh, God, Annmar-ie's coming back,'" she said. "Because they know I'll have some new thing for them to do."

"We know as (chief information officers) that we need to put these features in place, but we've gotten some push-back because it's a pain in the butt. Now that people see it happening in the real world, they're a little more accepting."

More valuable is instilling in employees a healthy skepticism in terms of what they click.

"I push 'delete' a lot," Stackpole said. "My approach to life at this point is – if that thing you sent me really needs to be clicked, you can make my phone ring."

JMURPHY7@Gannett. com

> *"I think ransomware is growing as an attack vector because it works and because people pay. The major issue at this point is that there's not really a good defense against it. It just takes one person to click something they shouldn't be clicking on."*
>
> *Bill Stackpole*
>
> *Professor of computing security at Rochester Institute of Technology*