

Sheldon ISD forced to pay nearly \$207K after hackers targeted servers

abc13.com/sheldon-isd-ransom-school-district-hacking-from-hackers-online/7036662

Jessica Willey

October 14, 2020

HOUSTON, Texas (KTRK) -- The Sheldon Independent School District paid nearly \$207,000 in ransom after hackers locked out officials from critical software systems last spring.

The ransomware attack happened in March. District officials could not access emails, important staff data or security cameras.

The Board of Trustees told ABC13 they were faced with a choice - pay 65 Bitcoins, which was equivalent to \$350,000 at the time, to regain access or lose everything and have to start over.

"Obviously, I'd certainly prefer not to pay the ransom," Sheldon ISD Superintendent Dr. King Davis said. "It would send a pretty strong message that we're not going to do it, but the reality is, for us to be functional, I just don't know how reasonable that is."

Rebuilding the district's system would take four to five months, which was explained during the emergency board meeting on March 19.

"We have our hands tied pretty bad here," one staff member said during the meeting.

In the end, the district, which is home to 10,000 students, negotiated and paid the hackers \$206,931. Its insurance company spent another \$100,000 on negotiations.

"After consulting with state and federal entities and our cybersecurity firm, paying was the best option to continue district operations effectively," the district said in a statement sent to ABC13.

Doug Levin, the founder of the Virginia-based K-12 Cybersecurity Resource Center, said the school districts hold a tremendous amount of data and its data criminals are interested in because they can monetize it.

He also added that the attack on school districts are on the rise and more disruptive than ever.

In 2019, there were 348 publicly disclosed incidents. Levin said 2020 is on the pace to exceed that number.

"When there is a cybersecurity incident now everyone is aware because teaching and learning stops," Levin said. "Before COVID-19, if there was a network issue, enterprising teachers could figure out ways to continue their lessons even without technology. That's just not simply possible right now without technology."

Levin said law enforcement never recommends paying ransom, even though districts are in a "lose-lose situation." The best defense is prevention.

"Being proactive with respect to cybersecurity is the way to go," Levin said. "It's definitely worth the money up front."

Sheldon ISD full statement on the incident:

"Sheldon ISD was able to work quickly to rebuild impacted systems after a security breach last school year in March. Throughout this time, Sheldon was transparent and communicated the effects from the breach. After consulting with state and federal entities and our cybersecurity firm, paying was the best option to continue district operations effectively. This provided Sheldon ISD with an opportunity to work toward continuous improvement by educating staff members about phishing attempts, conducting threat assessments and hardening network infrastructure."

Report a correction or typo

Related topics:

houstonhackingcyberattackmoneyteacherransomonline learningstudents

Copyright © 2022 KTRK-TV. All Rights Reserved.