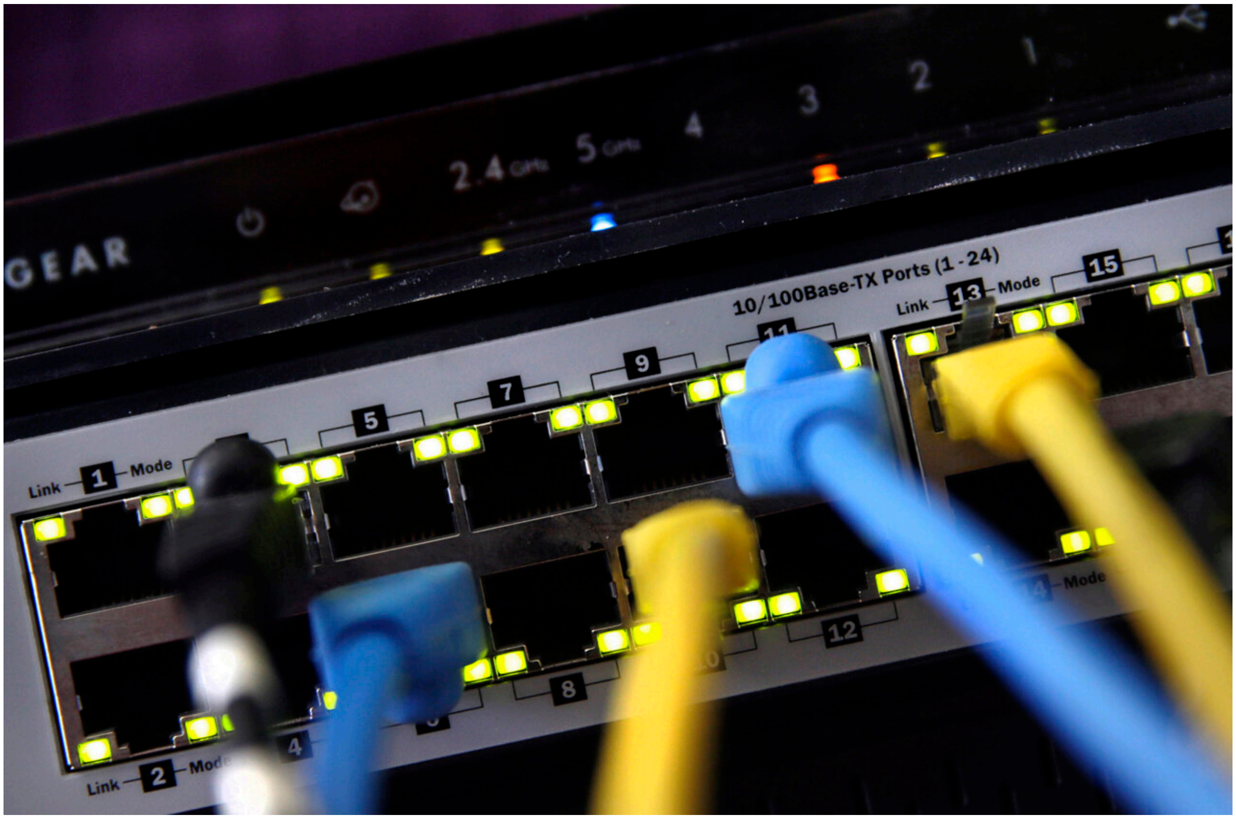
TechXplore

White House holds first-ever summit on the ransomware crisis plaguing the nation's public schools

August 8 2023, by Frank Bajak



In this June 19, 2018, file photo, a router and internet switch are displayed in East Derry, N.H. The White House on Tuesday held its first-ever cybersecurity "summit" on the ransomware attacks plaguing U.S. schools, which has included hackers leaking sensitive student data such as medical records, psychiatric evaluations and student sexual assault reports. Credit: AP Photo/Charles Krupa, File

The White House on Tuesday held its first-ever cybersecurity "summit" on the ransomware attacks plaguing U.S. schools, in which criminal hackers have dumped online sensitive student data, including medical records, psychiatric evaluations and even sexual assault reports.

"If we want to safeguard our children's futures we must protect their personal data," first lady Jill Biden, who is a teacher, told the gathering. "Every student deserves the opportunity to see a school counselor when they're struggling and not worry that these conversations will be shared with the world."

At least 48 districts have been hit by ransomware attacks this year—already three more than in all of 2022, according to the cybersecurity firm Emsisoft. All but 10 had data stolen, the firm reported. Typically, Russian-speaking foreign-based gangs steal the data—sometimes including the Social Security numbers and financial data of district staff—before activating network-encrypting malware then threaten to dump it online unless paid in cryptocurrency.

"Last school year, schools in Arizona, California, Washington, Massachusetts, West Virginia, Minnesota, New Hampshire and Michigan were all victims of major cyber attacks," the deputy national security advisor for cyber, Anne Neuberger, told the summit.

An October 2022 report from the Government Accountability Office, a federal watchdog agency, found that more than 1.2 million students were affected in 2020 alone—with lost learning ranging from three days to three weeks. Nearly one in three U.S. districts had been breached by the end of 2021, according to a survey by the Center for Internet Security, a federally funded nonprofit.

"Do not underestimate the ruthlessness of those who would do us harm," said Homeland Security Secretary Alejandro Mayorkas during the summit, noting that even reports on suicide attempts have been dumped online by criminal extortionists and urging educators to avail themselves of federal resources already available.

Education tech experts praised the Biden administration for the consciousness-raising but lamented that limited federal funds currently exist for them to tackle a scourge that cash-strapped school districts have been ill-equipped to defend effectively.

Among measures announced at the summit: The Cybersecurity and Infrastructure Security Agency will step up tailored security assessments for the K-12 sector while technology providers, including Amazon Web Services, Google and Cloudflare, are offering grants and other support.

A pilot proposed by Federal Communications Commission Chair Jessica Rosenworcel—yet to be voted on by the agency—would make $200 million available over three years to strengthen cyber defense in schools and libraries.

"That's a drop in the bucket," said Keith Krueger, CEO of the nonprofit Consortium for School Networking. School districts wrote the FCC last fall asking that it commit much more—Krueger urged that several hundred million be made available annually from its E-Rate program, which has helped expand broadband internet to schools and libraries across the country since 1997.

He said he was nevertheless heartened that the White House, Departments of Education and Homeland Security and the FCC recognize that the ransomware attacks plaguing the nation's 1,300 public school districts are "a five-alarm fire."

The lasting legacy of school ransomware attacks is not in school closures, multimillion-dollar recovery costs, or even soaring cyber insurance premiums. It is the trauma for staff, students and parents from the online exposure of private records—which the AP detailed in a report published last month, focusing on data theft by far-flung criminals from two districts: Minneapolis and the Los Angeles Unified School District.

Superintendent Alberto Carvalho of the Los Angeles district, the nation's second-largest, recounted for summit attendees lessons learned and best practices for mitigating the impact of extortionist ransomware attacks.

For starters, he said, "We don't negotiate with terrorists. We did not pay the ransom." Carvalho noted how the FBI told him that paying ransoms doesn't guarantee the stolen data won't eventually find its way onto dark web forums where hackers hawk it for use in ID theft, fraud and other crimes.

While other ransomware targets have fortified and segmented networks, encrypting data and mandating multi-factor authentication, school systems have reacted more slowly.

A big reason has been the unwillingness of school districts to fund full-time cybersecurity staff. In its 2023 annual survey, the Consortium for School Networking found that just 16% of districts have full-time network security staff, down from 21% last year.

Cybersecurity spending by districts is also meager. Just 24% of districts spend more than one-tenth of their IT budget on cybersecurity defense, the survey found, while nearly half spent 2% or less. —

Correction note: This story has been corrected to show the CEO's surname is Krueger, not Kroeger.

© 2023 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: White House holds first-ever summit on the ransomware crisis plaguing the nation's public schools (2023, August 8) retrieved 9 May 2024 from https://techxplore.com/news/2023-08-white-house-first-ever-summit-ransomware.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.