Why federal efforts to protect schools from cybersecurity threats fall short

December 14 2023, by Nir Kshetri

Credit: Pixabay/CC0 Public Domain

In August 2023, the White House announced a plan to bolster cybersecurity in K-12 schools—and with good reason. Between 2018 and mid-September 2023, there were 386 recorded cyberattacks in the

U.S. education sector and cost those schools $35.1 billion. K-12 schools were the primary target.

The new White House initiative includes a collaboration with federal agencies that have cybersecurity expertise, such as the Cybersecurity and Infrastructure Security Agency, the Federal Communications Commission and the FBI. Technology firms like Amazon, Google, Cloudflare, PowerSchool and D2L have pledged to support the initiative with training and resources.

While the steps taken by the White House are positive, as someone who teaches and conducts research about cybersecurity, I don't believe the proposed measures are enough to protect schools from cyberthreats. Here are four reasons why:

1. Schools face more cyberthreats than other sectors

Cyberattacks on K-12 schools increased more than eightfold in 2022. Educational institutions draw the interest of cybercriminals due to their weak cybersecurity. This weak cybersecurity provides an opportunity to access networks containing highly sensitive information.

Criminals can exploit students' information to apply for fraudulent government benefits and open unauthorized bank accounts and credit cards. In testimony to the House Ways and Means Subcommittee on Social Security, a Federal Trade Commission official noted that children's Social Security numbers are uniquely valuable because they have no credit history and can be paired with any name and date of birth. Over 10% of children enrolled in an identity protection service were discovered to have loans.

Cybercriminals can also use such information to launch ransomware attacks against schools. Ransomware attacks involve locking up a

computer or its files and demanding payment for their release. The ransomware victimization rate in the education sector surpasses that of all other surveyed industries, including health care, technology, financial services and manufacturing.

Schools are especially vulnerable to cyberthreats because more and more schools are lending electronic devices to students. Criminals have been found to hide malware within online textbooks and essays to dupe students into downloading it. Should students or teachers inadvertently download malware onto school-owned devices, criminals can launch an attack on the entire school network.

When faced with such an attack, schools can be desperate to comply with criminals' demands to ensure students' access to learning.

2. Schools lack cybersecurity personnel

K-12 schools' poor cybersecurity performance can be attributed, in part, to lack of staff. About two-thirds of school districts lack a full-time cybersecurity position. Those with cybersecurity staff often don't have the budget for a chief information security officer to oversee and manage the district's strategy. Often, the IT director takes on this role, but they have a broader responsibility for IT operations without a specific emphasis on security.

3. Schools lack cybersecurity skills

The lack of cybersecurity skills among existing staff hinders the development of strong cybersecurity programs.

Only 10% of educators say that they have a deep understanding of cybersecurity. The majority of students say that they have minimal or no

knowledge about cybersecurity. Cybersecurity awareness tends to be even lower in higher-poverty districts, where students have less access to cybersecurity education.

The Cybersecurity and Infrastructure Security Agency plans to provide cybersecurity training to an additional 300 K-12 schools, school districts and other organizations involved in K-12 education in the forthcoming school year. With 130,930 K-12 public schools and 13,187 public school districts in the U.S., CISA's plan serves only a tiny fraction of them.

4. Inadequate funding

The FCC has proposed a pilot program that would allocate $200 million over three years to boost cyberdefenses. With an annual budget of $66.6 million, this falls short of covering the entirety of cybersecurity costs, given that it will cost an estimated $5 billion to adequately secure the nation's K-12 schools.

The costs encompass hardware and software procurement, consulting, testing, and hiring data protection experts to combat cyberattacks. Frequent training is also needed to respond to evolving threats. As technology advances, cybercriminals adapt their methods to exploit vulnerabilities in digital systems. Teachers must be ready to address such risks.

Costs are sizable

How much should schools and districts be spending on cybersecurity? Other sectors can serve as a model to guide K-12 schools.

One way to determine cybersecurity funding is by the number of employees. In the financial services industry, for example, these costs

range from $1,300 to $3,000 per full-time employee. There are over 4 million teachers in the United States. Setting cybersecurity spending at $1,300 per teacher—the low end of what financial firms spend—would require K-12 schools to spend a total of $5 billion.

An alternate approach is to determine cybersecurity funding relative to IT spending. On average, U.S. enterprises are estimated to spend 10% of their IT budgets on cybersecurity. Since K-12 schools were estimated to spend more than $50 billion on IT in the 2020-21 fiscal year, allocating 10% to cybersecurity would also require them to spend $5 billion.

Another approach is to allocate cybersecurity spending as a proportion of the total budget. In 2019, cybersecurity spending represented 0.3% of the federal budget. Federal, state and local governments collectively allocate $810 billion for K-12 education. If schools set cybersecurity spending at 0.3%, following the example of federal agencies, that would require an annual budget of $2.4 billion.

By contrast, a fifth of schools dedicate less than 1% of their IT budgets—not their entire budgets—to cybersecurity. In 12% of school districts, there is no allocation for cybersecurity at all.

Provided by The Conversation