THE JOURNAL

Trends in Remote Learning: **Security & Connectivity**

The sudden advent of ubiquitous remote learning in K–12 has brought with it a range of challenges, not the least of which is the opportunistic increase in ransomware and other forms of malware targeting education environments.

SPONSORED BY: SONICWALL®

Table of Contents

K-12 Has Become the Most Targeted Segment for Ransomware

Malicious actors have disrupted remote learning by targeting school systems in their ransomware, malware and DDoS attacks. **BY DAVID NAGEL**

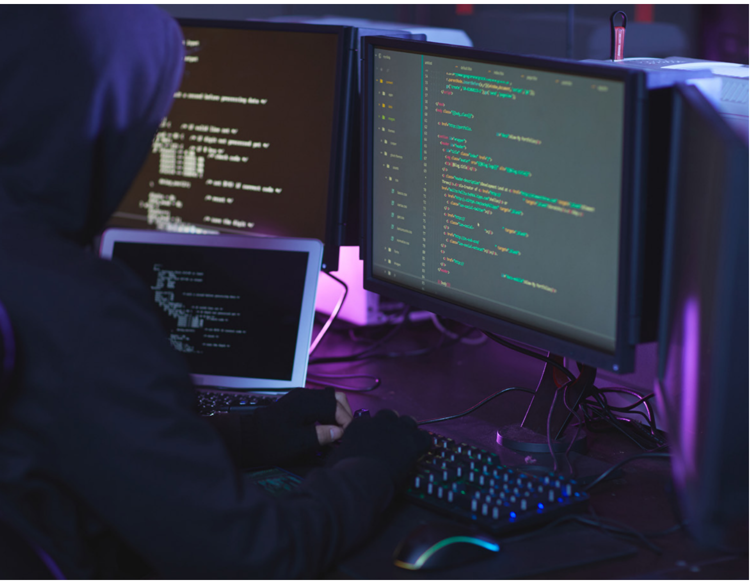
THE FBI AND OTHER FEDERAL SECURITY AGENCIES released a joint report that revealed an unsettling statistic for the 2020–2021 school year: the K–12 education segment has become not only the No. 1 target for ransomware since back-to-school, but it also makes up the majority of all ransomware attacks.

According to the report, 57 percent of all reported ransomware attacks in August and September were targeted at K–12, with actors exploiting the move to remote learning to cause disruptions. That's up from 28 percent for the period from January through July.

Ransomware is a form of malware in which the attacker gains access to the victim's computer systems and then holds the victim's systems and/or data for ransom. Perpetrators demand money on the threat of disabling computer systems that they've gained control over or releasing personal data they've stolen (generally private student data in the case of K–12 incidents).

The report, released Dec. 10, was created in a collaboration between the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC).

"The FBI, CISA, and MS-ISAC have received numerous reports of ransomware attacks against K-12 educational institutions. In these attacks, malicious cyber actors target school computer systems, slowing access, and – in some instances – rendering the systems inaccessible for basic functions, including distance learning. Adopting tactics previously leveraged against business and industry, ransomware actors have also stolen – and threatened to leak – confidential student data to the public unless institutions pay a ransom."



The FBI does not recommend paying ransoms. According to the report: "Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities."

According to the report: "The five most common ransomware variants identified in incidents targeting K-12 schools between January and September 2020 – based on open source information as well as victim and third-party incident reports made to MS-ISAC – are Ryuk, Maze, Nefilim, AKO, and Sodinokibi/REvil."

The FBI does not recommend paying ransoms. According to the report: "Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. However, regardless of whether your organization decided to pay the ransom, the FBI urges you to report ransomware incidents to your local FBI field office. Doing so provides the FBI with the critical information they need to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under US law."

Ransomware isn't the only bad news for K-12:

- **THE K-12 SEGMENT HAS ALSO BEEN TARGETED** for distributed denial-of-service attacks (DDoS), including third-parties providing support for remote learning.
- **THERE HAVE BEEN DISRUPTIONS OF VIDEOCONFERENCING SESSIONS,** including distance learning sessions, in which attackers join and disrupt classes by harassing, sharing images that are inappropriate for a classroom or even dox members of the audience (revealing sensitive information about them publicly). The report did not quantify these incidents.
- **OTHER FORMS OF MALWARE HAVE ALSO IMPACTED THE K-12 SEGMENT.** The most popular forms of malware used against K-12 institutions this year have included Shayler (39 percent of all malware used against K-12) and ZeUs (22 percent). Shayler, the most widespread, is the only malware in the top 10 that targets macOS. The report describes it as follows: Trojan downloader and dropper for MacOS malware.It is primarily distributed through malicious websites, hijacked domains, and malicious advertising posing as a fake Adobe Flash updater." The rest of the malware on the list target Windows operating systems.

The report offers several recommendations for network and security staff, as well as end users:

Network Best Practices

(bullet points verbatim from report)

- **PATCH** operating systems, software, and firmware as soon as manufacturers release updates.
- **CHECK CONFIGURATIONS** for every operating system version for educational institution-owned assets to prevent issues from arising that local users are unable to fix due to having local administration disabled.
- **REGULARLY CHANGE PASSWORDS** to network systems and accounts and avoid reusing passwords for different accounts.
- **USE MULTI-FACTOR AUTHENTICATION** where possible.
- **DISABLE** unused remote access/RDP ports and monitor remote access/RDP logs.
- **IMPLEMENT APPLICATION AND REMOTE ACCESS** allow listing to only allow systems to execute programs known and permitted by the established security policy.
- **AUDIT USER ACCOUNTS** with administrative privileges and configure access controls with least privilege in mind.
- **AUDIT LOGS** to ensure new accounts are legitimate.
- **SCAN FOR OPEN OR LISTENING PORTS** and mediate those that are not needed.
- **IDENTIFY CRITICAL ASSETS** such as student database servers and distance learning infrastructure; create backups of these systems and house the backups offline from the network.
- **IMPLEMENT NETWORK SEGMENTATION.** Sensitive data should not reside on the same server and network segment as the email environment.
- **SET ANTIVIRUS AND ANTI-MALWARE** solutions to automatically update; conduct regular scans.

End User Awareness Best Practices

(bullet points verbatim from report)

- **FOCUS ON AWARENESS AND TRAINING.** Because end users are targeted, make employees and students aware of the threats—such as ransomware and phishing scams—and how they are delivered. Additionally, provide users training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities.
- **ENSURE EMPLOYEES KNOW WHO TO CONTACT** when they see suspicious activity or when they believe they have been a victim of a cyberattack. This will ensure that the proper established mitigation strategy can be employed quickly and efficiently.
- **MONITOR PRIVACY SETTINGS** and information available on social networking sites.

The complete report is freely available at **ic3.gov**.

David Nagel is content editor for ***Campus Technology.***

Remote Learning Will Continue Growing over the Next Three Years

When it comes to delivering the "in-classroom experience" remotely, the focus has shifted to getting back to the basics. **BY DIAN SCHAFFHAUSER**

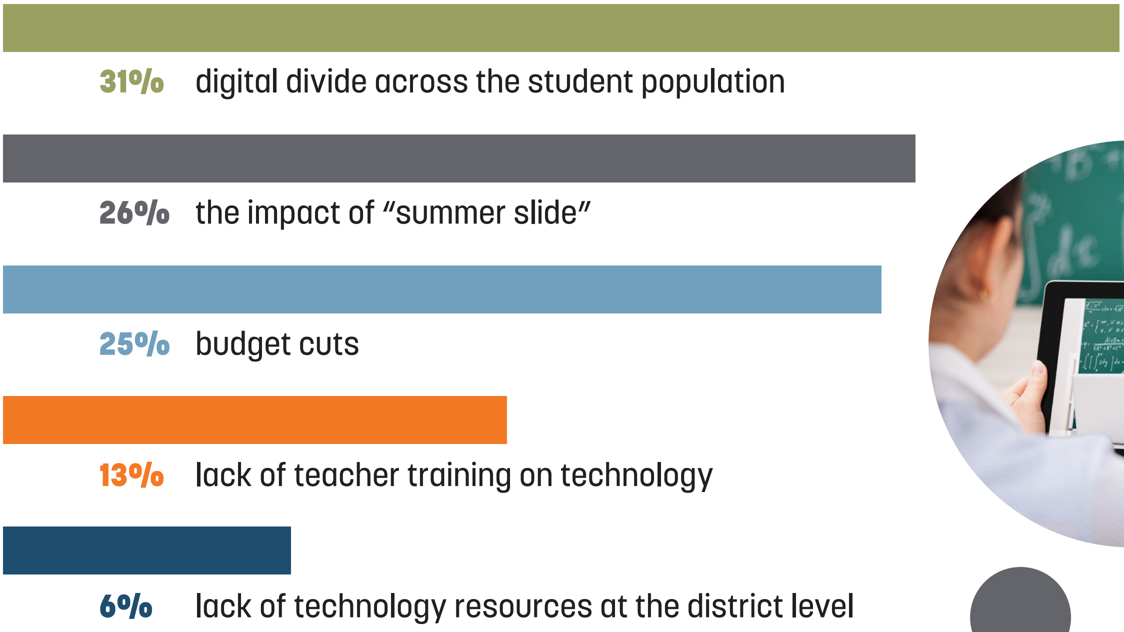
OVER THE NEXT THREE YEARS, a majority of K-12 educators expect online learning and digital curriculum to get ever more-important, while two STEM standbys will go by the wayside.

Sixty-three percent of respondents to a summer survey by interactive display company **Promethean** reported that they expect remote learning to experience the biggest growth, followed by virtual learning (54 percent) and the use of online content and resources (50 percent). But the use of robotics and coding has shrunk in importance, from choices selected by 49 percent in 2019 to 14 percent in 2020.

As the education technology company observed in a report on the results, perhaps "the focus has shifted to getting back to basics when delivering the in-classroom experience remotely."

Promethean commissioned a **survey** of 1,200 U.S. teachers and school leaders on a number of topics having to do with the state of technology in schools.

What are the challenges of teaching remotely?



A TEACHER RANKING OF PROFESSIONAL CHALLENGES IN REMOTE TEACHING.
SOURCE: **"THE STATE OF TECHNOLOGY IN EDUCATION 2020-2021 REPORT"** FROM **PROMETHEAN**

The survey found that the digital divide "runs deep." As one superintendent told researchers, "Equal access to the Internet when students are at home should be a priority for the state legislature."

The biggest barriers that surfaced for remote instruction, according to teachers specifically, was a lack of access to technology among students and engaging them. At the same time, half of all respondents (49 percent) said that the use of technology in the class was "a great way to engage students." As one teacher noted, "The biggest benefit of educational technology is that it mirrors how students learn outside of school."

Two-thirds of teacher respondents (69 percent) – both this year and last year – said they're "constantly striving to innovate by using technology as a tool for education." The remainder either feel that they use tech "competently" in their own lives but lack confidence to use it in school or "struggle" to use it at the level required for education purposes.

Maybe that's why when asked what schools needed to prioritize to make remote instruction successful, four in 10 survey participants (43 percent) said teachers needed training on the technology. A third (34 percent) reported that their schools had no "formal outlined strategy" for using tech.

"Technology continues to play a critical part in helping educators streamline learning and improve student outcomes," said Cheryl Miller, the company's chief marketing officer, in a statement. "As K-12 districts face a school year like none other, our 2020 'State of Technology' survey further demonstrates the need to make technology available to all districts and students to bridge learning gaps and help teachers create impactful learning experiences regardless of wherever those classrooms are taking place."

More complete results are available **with registration on the Promethean website.**

*DianSchaffhauser is content editor for **Campus Technology.***

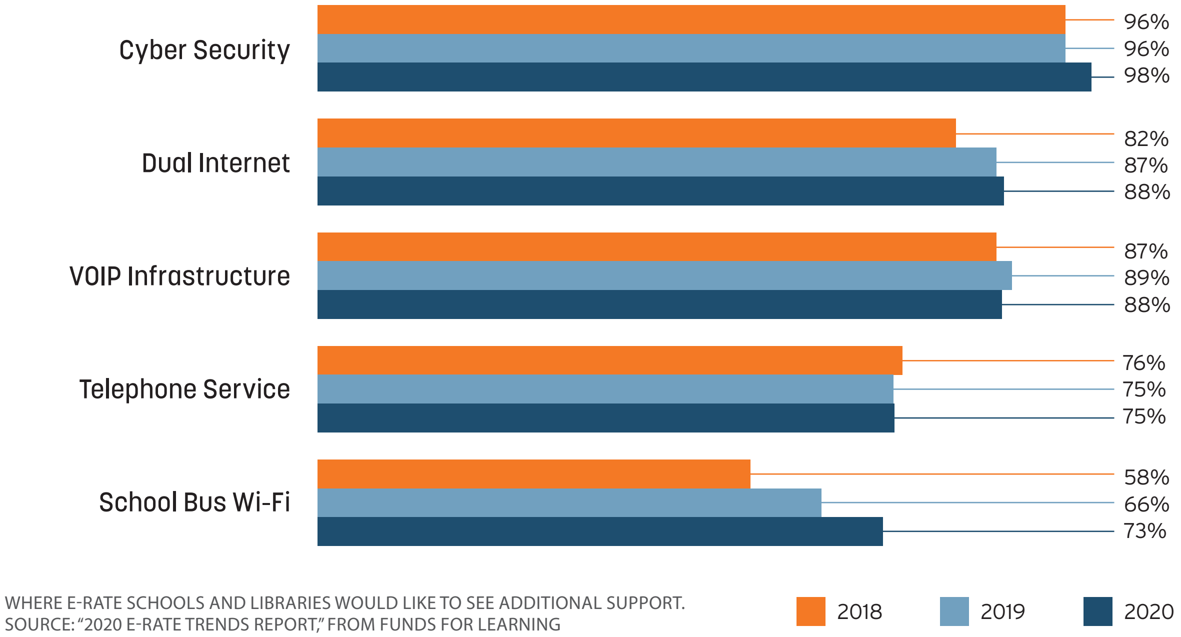
Survey Exposes Need for Off-Campus E-Rate Funding

The E-rate program supports most schools and libraries in the United States, providing billions of dollars annually to bolster the costs for internet access. **BY DIAN SCHAFFHAUSER**

IT'S TIME FOR E-RATE FUNDING TO SUPPORT off-campus connectivity too. That's a big theme in the latest survey by **Funds For Learning**, an E-rate consultancy. According to **a June 2020 survey** of 2,138 schools and districts that applied for E-rate, 90 percent of respondents reported that insufficient internet access was a significant issue in their communities. Ninety-three percent reported that they would share their discounted internet access for off-campus purposes if that were allowed by the **Federal Communications Commission**. And 82.5 percent agreed or "strongly" agreed that their schools and libraries would use the E-rate program for off-campus connections.

The E-rate program supports most schools and libraries in the United States, providing billions of dollars annually to bolster the costs for internet access, telecommunications and computer networking projects. The current program encompasses some 21,000 applicants and 4,100 vendors. The FCC runs the program through the **Universal Service Administrative Co**. E-rate funding is generated through fees collected from telecommunications customers.

Which of the following services should qualify for E-rate support?



WHERE E-RATE SCHOOLS AND LIBRARIES WOULD LIKE TO SEE ADDITIONAL SUPPORT.
SOURCE: "2020 E-RATE TRENDS REPORT," FROM FUNDS FOR LEARNING

One timely finding in the report was that most schools (59 percent) didn't or couldn't use any of the emergency relief funding they may have received from the federal government or their state governors earlier this year to expand connectivity off campus.

Also, the share of people who would like to see cybersecurity added as a qualifying E-rate service rose from 96 percent last year to 98 percent this year. The desire to see school bus WiFi added increased from 66 percent to 73 percent. And two-thirds would provision dual internet connections for more reliable connectivity if that were allowed by the FCC.

According to the company, E-rate continues to be a "vital program" in helping communities reach connectivity goals. Nine in 10 respondents agreed or strongly agreed that schools and libraries connected more students at faster speeds due to the E-rate program. "It would be devastating to our school without this program," one rural district respondent said. "Without the E-rate program we would not be able to provide internet access to our school," reported another.

For fiscal year 2019, the biggest Category 1 spending went to lit fiber, which drew $1.7 billion in expenditure. That was three times the amount spent for all other product types combined. For Category 2 spending, investments in switches and routers drew $726 million, followed by access points ($322 million) and cabling ($163 million).

Most respondents (59 percent) said they'd expect to upgrade their Wi-Fi network in the next one to three years. Twenty percent said it needed to happen within the next year.

"As the past few months have so poignantly demonstrated, an online connection should never be taken for granted. Internet access plays a central role in our society, and schools and libraries are at the forefront of making sure our communities are included online," said John Harrington, Funds For Learning CEO, in a statement. "The annual E-rate survey amplifies our combined voices to affect positive change for the program; we'll continue calling upon Congress to leverage the E-rate program for equitable off-campus internet connections."

The full report is openly available **on the Funds For Learning website**.

*DianSchaffhauser is content editor for **Campus Technology.***