United States Senate Committee on Health, Education, Labor and Pensions
Cybersecurity in the Health and Education Sectors.
Wednesday, May 18, 2022
10:00 a.m.
Testimony by Amy McLaughlin, Cybersecurity Program Director
Consortium of School Networking (CoSN)

Chairwoman Murray, Ranking Member Burr and Members of the Committee:

It is an honor to be with you today to talk about the cybersecurity threats and challenges facing K12 education. I'm Amy McLaughlin, I maintain multiple cybersecurity certifications including the Certified Information Systems Security Professional (CISSP), and Certified Information Systems Manager (CISM). I have over twenty years of experience as a cybersecurity professional that spans state and local government, K12 and higher education, and health care. I serve as the Cybersecurity Program Director for the Consortium of School Networking (CoSN) the national organization dedicated to meeting the needs of K12 education technology leaders.

These challenges were daunting before the COVID-19 pandemic, and the rapid deployment of millions of one-to-one mobile devices to shift schools to remote and hybrid learning expanded the technology footprint and increased opportunities for malicious attacks.

The threats faced by K 12 schools and the education sector are very serious and constantly changing. Gone are the days where cyber threats came from individual "script kiddies" who sought to access systems, write viruses and worms just to see if they could. Today's cyber threats come from organized crime, nation state actors, and terrorist organizations[1] who have three objectives - use cybercrime to make money through ransoming data or stealing and selling data, collecting data for future use, and disrupting U.S infrastructure and daily life with attacks on our ability to offer a free public education. In addition to external threats, education faces internal threats from students who can quickly and easily learn how to buy or conduct disruptive attacks online.

Attacks against the K12 system are increasing. In December 2020, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) issued a TLP:WHITE level Joint Advisory[2] identifying K12 as targets of opportunity for cyber actors and identified increased attacks against education organizations.

The increase in attacks is reflected in the data around ransomware attacks. The 2020 Joint Advisory cited the MS-ISAC data indicating that "the percentage of reported ransomware incidents against K-12

[1] https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions
[2] https://www.cisa.gov/uscert/ncas/alerts/aa20-345a

schools increased at the beginning of the 2020 school year. In August and September, 57% of ransomware incidents reported to the MS-ISAC involved K-12 schools, compared to 28% of all reported ransomware incidents from January through July." This trend continued into 2021 and continues to be a significant issue going into 2022. Bad actors do not discriminate by location. Cyberattacks hit the biggest urban and suburban school districts as well as the smallest rural schools.

Our K12 schools and districts recognize the serious privacy, monetary, and operational significance of the cyber threats. CoSN's 2022 Ed Tech Trends report identified cybersecurity as the top unmet technology need stating that "even before the pandemic required schools to move more services online, cybersecurity has been a top concern for districts. In a situation where even well-funded corporations in the private sector struggle to address cybersecurity issues, poorly funded districts are at a disadvantage. One respondent called the need for more cybersecurity funding as "desperate."

Cybersecurity is not only an unmet technology need; it is an organizational culture challenge. K12 organizations are vulnerable to cyber actors who leverage phishing attacks and social engineering skills to attack school systems with ransomware and other malware or obtain login credentials to access and hack systems. These attacks exploit the helpful and service-oriented focus of school staff and teachers to perpetrate malicious attacks. School district technology leaders work to help staff and teachers recognize these tricks but cybersecurity education must become a more systemic part of educator preparation and professional development and other staff training.

There are many cybersecurity threats facing K-12 schools. In lieu of providing an exhaustive list, I'll share with you the most prevalent threats:

Ransomware and other malware attacks are often the most destructive and disruptive threat facing education. Ransomware is malicious software designed to encrypt files and block access to computer systems until a sum of money is paid. The more advanced forms of ransomware not only encrypt files, they also exfiltrate the files to the attacker who can then hold the data hostage, resell the data on the dark web, or collect the data for later uses that are, as yet, unknown and, in the case of data stolen by nation state actors, may become a national security threat. Just to be clear, these bad actors are stealing the most damaging and sensitive student, family, employee, and district financial data held by school districts and disseminating it to the highest bidder.

The State of Louisiana experienced the devastating impact of ransomware in 2019 when Louisiana's governor had to declare a state of emergency after a series of cyber- attacks shut down phones and locked and encrypted data at three of the state's school districts[3]. The attack disrupted teaching and learning and ransomware response ultimately cost the state over $2.3 million[4]. 75,000 students in Albuquerque, NM missed two days of school in a 2022 ransomware attack[5].

[3] https://www.cnbc.com/2019/07/26/louisiana-declares-state-of-emergency-after-cybercriminals-attack-school-districts.html
[4] https://www.theadvocate.com/baton_rouge/news/politics/legislature/article_caf129ae-5e62-11ea-912b-77e0d8405441.html
[5] https://www.usnews.com/news/best-states/new-mexico/articles/2022-01-18/albuquerque-schools-confirm-ransomware-attack-resume-class

Second, education is inundated with ongoing phishing attacks through school district and other email systems. Phishing is an attack that leverages sending fraudulent emails purporting to be from reputable companies and organizations in order to trick individuals to reveal personal information, such as passwords and credit card numbers or send data directly to the cyber actor for example, W2 forms and gift card numbers. "Phishing attacks are responsible for more than 80% of reported security incidents. According to CISCO's 2021 Cybersecurity Threat Trends report, about 90% of data breaches occur due to phishing. Spear phishing is the most common type of phishing attack, comprising 65% of all phishing attacks. The 2021 Tessian research revealed that employees receive an average of 14 malicious emails every year".[6]

Third, schools are frequently victims of (DDOS) distributed denial of service attacks. DDOS attacks occur when multiple machines are operating together to attack one target, they flood the target network, server or system, with traffic and illegitimate activity disabling the systems and making them inaccessible. As the FBI, CISA, MS-ISAC Joint Advisory noted, the availability of DDoS-for-hire services provides opportunities for any motivated malicious cyber actor to conduct disruptive attacks regardless of experience level, including students. Miami-Dade School District experienced a particularly disruptive DDoS attack in September 2020 that impacted the districts ability to offer 200,000 students remote learning for the first two days of the school year[7]. This attack was perpetrated by a 16-year old high school junior[8].

A less obvious, but large threat to K12 schools, are cyber-attacks against third party companies that provide essential operational and instructional technologies . Many K12 school systems leverage software as a service providers and cloud hosted systems to deliver important technologies for supporting teaching, learning and the delivery of school services including student information systems, learning management systems, ERP systems for finance and human resources, and more. Attacks against third party services providers can result in wide scale outages for schools and widescale data theft or data destruction. Examples of vulnerable and exploited third-party tools that have impacted K12 education include the 2020 SolarWinds hack[9], the 2021 Log4J vulnerability that had organizations scrambling to identify vulnerable systems and remediate them[10], and the 2022 data breach at Illuminate Education which impacted at least 24 districts[11].

Additional threats include social engineering, end of life and unsupported software and operating systems, open and exposed Internet of Things (IoT) systems, video conference disruptions, website defacement and hacktivism, and more.

The impacts of cyberattacks on K12 school systems are extensive. Students are directly impacted by lost instructional time when schools are closed as a result of ransomware or other debilitating

[6] https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/
[7] https://thehill.com/policy/cybersecurity/514802-miami-dade-school-district-virtual-classes-disrupted-by-cyberattack/
[8] https://www.nytimes.com/2020/09/03/us/miami-dade-school-cyberattack.html
[9] https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/
[10] https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
[11] https://thejournal.com/articles/2022/05/03/illuminate-education-data-breach-impacted-at-least-24-districts-18-charter-schools-in-ny.aspx

attacks. Successful cyberattacks damage the reputation of schools and undermine trust of students and parents in the ability of school districts to protect student data and maintain consistent services. Cyberattacks are a crime, yet school districts who are victimized by these sophisticated criminal operations face blame for the crime.

The cost of responding to a cybersecurity incident, restoring systems, and providing services to impacted students and staff is high. In 2021, the average data breach by in the education sector costs $3.79 million[12]. The cost per individual record lost to a data breach can exceed $165 per record. These costs roll over to other schools and districts as insurance companies raise cybersecurity premiums and deductibles. Cybersecurity insurance costs for K12 are rising by 25-300% with more limited coverage and high deductible[13].

School districts across the country are facing rising insurance costs regardless of whether they have had a cybersecurity incident or not. Not only are insurance premiums increasing, the ability to even become insured has now become predicated on successful completion of a risk assessment and implementation of specific cybersecurity safeguards. The costs of new cybersecurity safeguards and rising insurance premiums prices many school districts out of the insurance market.

There are individual financial and psychological impacts to staff and student victims of cybersecurity attacks. Individuals whose identities are stolen face financial hardship from the loss of their personal data, and students whose identities are stolen may not realize the full financial impact until much later. Since 2017 there has been a growing trend of sales of student data on the dark web. Identities of students who are too young to have existing credit accounts are valuable commodities.

Students under 18, without existing credit accounts, have found themselves victims of identity theft and credit card fraud when stolen data is used to open accounts using their information. Often the fraudulent accounts go undetected until students apply for financial aid for college, or attempt to obtain credit for the first time only to discover their credit is destroyed and their finances are crippled by data theft from a previous cyber-attack.

Data breaches and identity theft also result in mental health impacts. According to a recent survey by the nonprofit Identity Theft Resource Center, " 86% of identity theft, victims reported feeling worried, angry and frustrated, nearly 70% felt they could not trust others and felt unsafe, and nearly 85% reported disturbances in their sleep habits and 77% reported increased stress levels, and nearly 64%, they had trouble had trouble concentrating."

---

[12] Cost of a Data Breach Report 2021, IBM Security https://doc-0k-5g-apps-viewer.googleusercontent.com/viewer/secure/pdf/pp9sepf14apgmvrtn4gr78ef7erikjgp/ke3i7gc3usr03dhfesplfnjgpfsrg4d1/1652374200000/drive/14468447276760910654/ACFrOgDH7U4d_azWxsl9zUMG_du0g1d1xPAzRyNRZOZ80u9mK7921h7ZxHLm0C2HHrjSTa_LsSLDcpD_iREpwtCR4j_9Y6RT8Kdpooo7pTum8mhiQ9IZ0kRnnJtex2inBASkqwbNCRUozGq4Vg1B?print=true

[13] https://www.businessinsurance.com/article/20220216/NEWS06/912347780/Perspectives-New-lessons-for-K-12-schools-on-cyber-security,-insurance-cover-#:~:text=K%2D12%20schools%20face%20a,deductibles%20and%20narrower%20coverage%20terms.

K-12 schools and districts experience significant challenges in protecting themselves from cyberattack. First, school districts are not funded to purchase in depth cybersecurity technologies to safeguard their systems and data. These technologies are expensive and existing mechanisms funding high speed internet access, such as the E-rate program, do not fund network defenses.

Staffing and the ability to hire cybersecurity professionals is another challenge school districts face. There are not enough cybersecurity professionals available and school districts can't afford them. According to , "Only a fifth (21%) of districts have a full-time equivalent (FTE) employee dedicated to network security, the same percentage as the prior year. This means that cybersecurity protection is a part-time responsibility in a large majority of school districts… In lieu of a full-time cybersecurity position, districts address cybersecurity in a variety of ways. A third (33%) of districts include the responsibility as part of another job."

Today there are almost 500,000 unfilled cybersecurity positions in the United States that number is projected to increase. School districts struggle to find qualified cybersecurity staff who will work for a K-12 salary. The competition for skilled cybersecurity professionals also results in districts making tough choices between hiring one or two teachers or hiring a cybersecurity professional.

Ensuring cybersecurity equity in education is a significant challenge. Every school district faces cybersecurity threats, but they disproportionately impact school districts with less funding available to staff, support, and secure their technologies. Often, rural, and low-income schools and districts have less funding available to hire dedicated expert staff and maintain their technology up-to-date resulting in higher risk of unsupported and aging systems vulnerable to attack.

Recognizing the many attack vectors and challenges they face, K-12 school systems are taking many steps to improve and expand protections for data and IT systems. The 2022 CoSN Ed Tech Leadership Survey identified the following steps being taken to protect data and systems:

- 65% of schools and districts responding to the survey focusing on IT staff training to help grow the skills of their staff in the cybersecurity space. In lieu of hiring trained cybersecurity professionals, districts are seeking to grow these skills internally.
- 63% are investing in end-user training which can address the
- 55% are leveraging off-site backups which is the number one step districts can take to be able to recover quickly from a ransomware attack.
- 54% were working with staff to upgrade their passwords to expand from a basic eight-character password to a stronger passphrase of at least 12 characters. Increasing the number of

characters in a password from eight to twelve characters increases the time a supercomputer needs to brute-force crack a password from minutes to centuries[14].

There are additional steps that can be taken at a national level to help schools and districts improve cybersecurity defenses and services across the country.

1. Update E-rate's definition of firewall to encompass next-generation firewalls and services. CoSN[15] filed a petition with the Federal Communications Commission in 2021 requesting this change. This does not require legislation and the FCC can and should immediately take this action.
2. Encourage the the U.S. Department of Education through the Privacy Technical Assistance Center to expand guidance materials and coordinate services across federal agencies to provide a comprehensive menu of products.
3. Support the implementation of Rep. Matsui's 2021 Enhancing K-12 Cybersecurity Act[16], which CoSN has endorsed.
4. Fund MS-ISAC to provide their fee-based services to K12 free of charge and expand staffing of their Security Operations Center.
5. Fund university and college run Security Operations Centers (SOCs). Colleges and universities are developing non-profit SOCs offer cost-effective services for K12 schools and train new cybersecurity professionals increasing the number of people capable of filling open positions.
6. Help schools hire expert staffing.

Our K12 school districts are on the front lines of protecting their data and systems against much larger, better funded organizations, and a rapidly evolving cyber threat environment. To borrow a quote from "Hamilton" they are "outgunned, outmanned, outnumbered, out planned." They need access to staffing and technical resources to continue to securely deliver on the mission of delivering education.

[14] Firewalls Don't Stop Dragons, Fourth Edition, Cary Parker, Apress, p.109.

[15] http://d31hzlhk6di2h5.cloudfront.net/20190903/cc/f3/72/41/228e09116606c764f2d2f2c4/CoSN_Cat_Two_Filing_Final_2019.pdf

[16] https://www.congress.gov/bill/117th-congress/house-bill/4005?q=%7B%22search%22%3A%5B%22hr+3%22%5D%7D&s=1&r=64