School Safety Newsletter

Volume 6, Issue 11 June 2019

Survey: What School District Tech Leaders are Saying About Cybersecurity

Education Week, March 19, 2019

https://www.edweek.org/ew/articles/technology/2019/03/20/rural-school-districts-lag-behind-in-cybersecurity.html

District tech leaders have different concerns about cybersecurity, and different strategies for addressing those concerns, which vary by the size of their school systems. Compared to their rural counterparts, administrators from big-city districts are more likely to say their worries about protecting their K-12 systems are on the rise—and they're more likely to have begun implementing formal password-management policies and measures.

That's according to a survey conducted by the Consortium for School Networking and the Education Week Research Center of more than 300 ed-tech leaders.

Overall, 68 percent of leaders say that student-data privacy and security is a somewhat or much more important priority this year compared with last year.

That share rises to 82 percent for administrators from urban school districts. By comparison, it's 68 percent for suburban leaders and 64 percent for their rural peers.

This is not to say that student data privacy and security are unimportant to leaders from rural districts. They may have more basic concerns—like accessing the internet in the first place. Even as the percentage of U.S. schools with WiFi skyrocketed from 30 percent to 98 percent between 2013 and 2018—according to data from the nonprofit EducationSuperHighway—many rural schools continue to face challenges merely getting connected.

But within the biggest K-12 systems, cybersecurity is seen as an urgent problem.

One hundred percent of leaders from large districts with more than 50,000 students report that student data privacy and security is a somewhat or much more important priority this year compared with last year. That percentage falls to 63 percent for those from small districts with fewer than 1,000 students.

Across the country, worries about cybersecurity among tech leaders from districts of all sizes have soared over the past few years, notes Keith Krueger, the chief executive officer of the Consortium for School Networking. But the challenges that rural school systems face in protecting themselves from cyber threats are especially acute, he said.

If the largest school K-12 districts are scrambling to keep up, "one can only imagine the challenge for small school systems with no technical staff," Krueger explained. "The best you can do is [find out] what best practice is, implement that, and make sure your school board and your superintendent understand that these are the steps worth taking—and that even with those best steps, bad things can happen."

Shunning Password Protections

All districts face hurdles in responding to threats and in creating safeguards that are both effective and reasonably easy to manage, said Keith Bockwoldt, the chief information officer for the 4,500-student Hinsdale High School District in Illinois.

Protecting our future through information sharing

In This Issue

Survey: What School District Tech Leaders are Saying About Cybersecurity (Continued)

Larger systems, for instance, face more complex challenges in protecting data and training staff because of their size and getting everyone on board with their policies, said Bockwoldt, who serves on CoSN's cybersecurity advisory committee.

"The threats are there, whatever classification you're in," Bockwoldt said. In that sense, "everyone is in the same boat."

Concerns about student data privacy and security are not the only aspects of cybersecurity in which large and urban district leaders differ from their small and rural peers.

Large and urban leaders also approach password management differently than do their peers from smaller, rural and suburban districts.

For example, just over half (56 percent) of all K-12 leaders say their districts have formal password policies that are widely followed. Seventy-two percent of urban leaders say they have widely-followed formal password policies. That's compared with 62 percent of suburban administrators and less than half (41 percent) of their rural counterparts. In fact, nearly 1 in 3 (29 percent) of rural leaders report that their districts do not have formal password policies although staff members are regularly encouraged to use best practices for password management.

'This Is Crazy'

Timothy Smith, the supervisor of instructional practice and technology integration for the Red Lion Area School District in Pennsylvania, said tech leaders in rural K-12 systems may have a harder time than their urban peers imagining that malicious actors will target their schools.

District officials in smaller districts may think, "Why would they focus on me? Why would there be a hacker or someone who wants to dig into the data that we have?" said Smith, whose district has 6,100 students.

Smaller districts are much less likely to have full time chief technology officers than larger districts, according to federal data. Because rural tech leaders are juggling so many duties, making progress on even relatively simple cybersecurity steps can be difficult, said Smith.

Despite those odds, his district has taken steps to tighten the security reins. Three years ago, his school system put in place stronger protocols for password security. Smith had assumed everyone would be on board with the measure, but he still gets resistance.

"I was really surprised by that," he said. "Every 120 days, without fail, I will get one or two or three staff members who will reach out to me and say this is crazy [to change passwords]."

'Protect Data at All Costs'

The COSN/EdWeek survey found that 100 percent of large district leaders have formal, widely-followed password policies. That share falls to 43 percent for administrators from small districts.

In addition to examining formal password policies, the survey also asked leaders if their districts had implemented 13 different types of security measures related to passwords, including requiring passwords to be of minimal complexity and/or length (84 percent); prohibiting password sharing (73 percent) and locking accounts after a specified number of unsuccessful log-in attempts (62 percent). Urban leaders are more likely than their rural or suburban peers to have implemented 11 of the 13 measures. For example, 96 percent of urban leaders say they require minimum lengths and levels of complexity for passwords, compared with 86 percent of suburban respondents and 76 percent from rural areas.

Similarly, 87 percent of urban respondents said their districts prohibit password sharing, compared with 78 percent of suburban leaders and 66 percent of their rural counterparts. Leaders from larger districts are also more likely than those from the smallest districts to report that they had implemented the 13 security measures.

For many districts, no matter what their size, effective cybersecurity means thinking differently about the obligations they have to protect students, said Smith. Just as schools establish physical barriers to make sure access to their campuses are controlled, he argued, "we need to be the beacon that will protect data at all costs."

Eanes Independent School District Parents Outraged Over Tablet Security

Spectrum Local News, May 7, 2019

https://spectrumlocalnews.com/tx/austin/news/2019/05/08/eanes-isd-parents-outraged-over-tablet-security

WEST LAKE HILLS, Texas — Meaghan Edwards keeps a close eye on how much screen time her kids get at home, but after a phone call back in March, she wants to limit screen time at school, too.

- Parents concerned about explicit content on school-issued tablets
- Eanes Independent School District (EISD) says several layers of filters are already on tablets
- Other parents had similar complaints last fall

“You’ve got to come here immediately something terrible has happened. Can you come to the classroom?” recalls Edwards.

Meaghan’s first grade son was discovered using a voice command to search his school-issued tablet.

"He had been accessing pornographic images through a google search,” she said.

In an email, a spokeswoman for the Eanes Independent School District insists there were several layers of web filters on the tablet already in place.

“Since we have been a 1:1 district for eight years, we have learned, we have taken feedback from parents and we have made changes along the way. In this particular case, there was not a security breach. The student was actively searching for mature adult content, and while we have several layers of web filtering technologies, not every search engine is completely foolproof,” Claudia McWhorter, Executive Director of Communication and Community Engagement at the EISD said via email.

Since this incident, the district insists it has tightened restrictions on student access.

Meaghan says it’s too little, too late.

“We thought we were a long way off from having to talk about pornography at home,” Edwards said.

In a statement, the district says the following protocols are in place:

- Block social media, pornography, mature, dating and instant messaging forums, security, violence, advertisements and online shopping
- Block access to the Apple app store and only approve instructionally approved apps
- Maintain a primary in-district web filter for grades K-12
- Block the Google Search images tab for grades K-5
- Added a second in-district web filter for grades K-5
- Turned on keyword filtering district-wide to block any search result for mature content
- Reinforce expectations for teacher supervision and use of classroom technology

Edwards still places the blame on the district.

“I didn’t want him to think we were mad at him because he’s curious. He’s a child,” she said.

Edwards said the district already knew about these vulnerabilities, and she's not the only parent having difficult conversations. A public document , put together by an Eanes ISD task force, shows similar complaints from other parents last fall.

“I’m outraged. I cannot believe that this is not an isolated incident,” Edwards said.

For the district’s part, the task force continues to serve a vital purpose.

“We have listened to parent feedback over the years - including feedback from the Digital Learning Task Force - and have made improvements throughout the years. It is a constant process as technologies evolve - both on the side of getting through our filters and on the side of implementing solutions to stop those getting through our filters.

Eanes Independent School District Parents Outraged Over Tablet Security (Continued)

We were aware of a few cases in the past and were thankful for the work of the DLTF to bring those to light. Since the formation of that task force in 2015, in the spirit of transparency, we made all notes and parent feedback available to the public. Most of the incidents we had already addressed when they happened, and they helped improve our system. We are saddened that a parent would use those notes and feedback as criticism since the strength of our program has been built around parent feedback and teacher leadership.

Of note, we are nationally recognized as a vanguard district when it comes to educational technology and have four campuses (including the one where the incident occurred) recognized as an Apple Distinguished School for its thoughtful approach to technology integration," McWhorter said via email.

Eanes ISD also sent out a letter to parents about its plans to update technology in the classroom and make it more secure.

Now, Edwards and roughly 200 other parents have signed a petition asking for fundamental changes to these devices in the classroom, starting by giving parents the choice to opt-out of tablet use.

"I want a classroom without iPads for my sons," Edwards said.

Other parents, some of whom didn't want to go on camera, said tablets aren't supplemental tools anymore, instead they fear the tablets are being used as rewards.

"We walk into these classrooms and the kids are just glued to the screens," Edwards said.

Several parents are now preparing to go before the school board on May 21 to deliver the petition and appeal directly to trustees and the superintendent.

Edwards says she'll continue working for a change.

"We want our children protected at school," she said.

Police: 12-year-old Girl Made 'Suicide Pact' with Snapchat Predator

WAND 17, May 30, 2019

https://www.wandtv.com/news/police--year-old-girl-made-suicide-pact-with-snapchat/article_3b6b16ba-82de-11e9-942a-2743a68ede93.html

CHATHAM, Il - It is ever parent's worst nightmare, an online predator convincing their child to send sexual photos and even self-harm.

Chatham Police said a family may have come close to losing their 12-year-old little girl.

They are calling it a social media horror story.

The girl's mother came to police after discovering a predator was using the app Snapchat to prey on her daughter. Snapchat is a messaging app where pictures that are sent disappear after several seconds. It can also be used to send text messages.

The girl's mother saw a change in her behavior and noticed her school work was starting to suffer.

She learned a predator was convincing her child to send nude photos of herself and was grooming her to self harm.

The predator had even made a "countdown" agreement where they were both supposed to commit suicide together.

The mother told police she felt her daughter would have followed through with this based on her actions leading up to it.

"It is easier than most parents think for predators to gain access to children via social media," police warned parents. "Please, monitor your child's chat conversations and who they are communicating with."

Three United States Universities Disclose Data Breaches Over Two-Day Span

Bleeping Computer, June 15, 2019

https://www.bleepingcomputer.com/news/security/three-us-universities-disclose-data-breaches-over-two-day-span/

Three U.S. universities have disclosed data breach incidents impacting personally identifiable information of students or employees following unauthorized access to some of their employees' email accounts.

Three United States Universities Disclose Data Breaches Over Two-Day Span (Continued)

All three universities — Graceland University, Oregon State University, and Missouri Southern State University — have notified the individuals whose personal information was potentially stolen or accessed about the security incidents.

In addition, no evidence has been found of the impacted personal information being stolen or used in a malicious manner while investigating the disclosed data privacy incidents involving all three universities.

Graceland University says in a notice of data breach published on June 14 that an "unauthorized user gained access to the email accounts of current employees," on March 29, 2019, as well as "from April 1-30 and April 12-May 1, 2019, respectively."

As the university discovered during the breach investigation, "the personal information of some people who had interacted with these email accounts over the past several years was available during the time the unauthorized user(s) had access."

The information that could have been accessed during the incident contained:

- full name
- social security number
- date of birth
- address
- telephone number
- email address
- parents/children
- salary information
- financial aid information for enrollment or possible enrollment at Graceland

Oregon State University (OSU) states in a press release that "636 student records and family records of students containing personally identifiable information were potentially affected by a data privacy incident that occurred in early May."

OSU says that a joint investigation carried out with the help of forensics specialists found that an employee's hacked email account containing documents with the info of the 636 students and their family members was also used by the attackers to "send phishing e-mails across the nation."

As detailed by Steve Clark, OSU's VP for university relations and marketing:

OSU is continuing to investigate this matter and determine whether the cyber attacker viewed or copied these documents with personal information.

According to Clark, the university is also reviewing the protection systems and procedures used to shield OSU's e-mail accounts and information systems.

Missouri Southern State University (MSSU), the third entity which reported a breach, states in a notice of data breach sent to the Office of the Vermont Attorney General that it was alerted of a possible cyber attack triggered by a phishing email on January 9.

The phishing attack made several victims among the university's employees which prompted a law enforcement notification. The university officials were told afterward to delay notification of affected individuals until investigations are complete.

MSSU also hired a leading forensic investigation firm to look into the security incident and to "block potential email exploitation, including a mass password reset of all employee Office 365 accounts."

After analyzing the contents of the impacted Office 365 accounts, MSSU found that the emails contained within stored "first and last names, dates of birth, home addresses, email addresses, telephone numbers, and social security numbers."

As further explained in the data breach notification send to the Vermont Attorney General by MSSU:

In late March, April, and early May, the University identified emails containing personal information that may have been compromised by the attack. In mid-May, the University confirmed that your first and last name and social security number were contained in the impacted accounts.

BleepingComputer has reached out to Graceland University, Oregon State University, and Missouri Southern State University for additional comments, but had not heard back at the time of this publication.

Update June 17: Mike Olmstead, Missouri Southern State University's Director of News Services & Messaging, sent an official statement from the university:

Three United States Universities Disclose Data Breaches Over Two-Day Span (Continued)

Missouri Southern State University was the victim of a cybersecurity attack on January 9, 2019. The University responded quickly and engaged a leading forensic investigation firm to help stop the attack and provide subsequent investigation services. The University notified the Federal Bureau of Investigation Cyber Crime Task Force and the Missouri Attorney General's Office about the incident. The University worked diligently to notify all impacted individuals once the results of its investigation had been communicated to law enforcement. The notification letters were mailed to all impacted individuals on June 13, 2019, and the University has offered all impacted individuals 24 months complimentary credit monitoring.

Anonymous Colorado School Safety Line Sees Record Number of Tips in May

Colorado Independent, June 7, 2019

https://www.coloradoindependent.com/2019/06/07/colorado-school-safety-anonymous-hotline/

A state program that allows students to anonymously report concerns for their own safety or the safety of others in Colorado schools received a record number of tips this May, a sign, some say, that students are feeling more empowered to keep their schools safe.

The Safe2Tell program, which started in 2004 and was adopted by the state Attorney General's office around five years ago, announced in its May report that the program received 2,877 tips last month alone.

This is an 84% increase in monthly tip volume compared to May of last year, the largest increase the program has seen since being picked up by the Attorney General's office, said Program Director Essi Ellis.

"I truly believe it is students wanting to make a difference within their schools and really help their peers," Ellis said, adding, "Even if we can help one student in need or in crisis, we feel that as a victory for the program."

Safe2Tell gives students, parents, school staff and community an anonymous way to report safety concerns. Tips can be submitted online, over the phone or through the Safe2Tell app.

Submitted tips are screened by the eight Safe2Tell data analysts, who are trained to receive and disseminate these tips to local law enforcement and school administrations.

The service has been used before to address violent threats and possible suicidal actions within schools. In the 2018-2019 school year, Safe2Tell reported it had received 18,916 actionable, or serious, tips, a 22% increase over the previous school year. Suicide, drugs and bullying are consistently the top three categories reported to the program. Suicide threats alone increased 68% since May of 2018, according to the report.

These numbers come just a month after a deadly shooting at the STEM School in Highlands Ranch that killed one and injured eight. School shooting like these, as well as others around the country, can lead to more calls in the future, Ellis said.

"I think it is students breaking that code of silence and really wanting to speak up and empower themselves and their peers to really protect their school," she said.

According to the release, law enforcement and school districts reported that 97.5 percent of tips were submitted in "good faith" and 2.45 percent of the tips were false this school year.

School Safety Newsletter

Statewide Terrorism &
Intelligence Center
2200 S. Dirksen Parkway
Springfield, IL 62703
Phone: 217-558-2661
E-Mail:
Isp.schoolsafety@illinois.com

Mia A. Ray
School Intelligence
Officer