Ramping Up Your Cybersecurity

Education leaders explore the importance of and path to cybersecurity.

By Keith R. Krueger, CAE; James M. Rowan, CAE, SFO; and David R. Schuler, PhD

MZ/STOCK.ADOBE.COM

It's Thursday afternoon. Someone sitting at the coffee shop on the corner of 5th and Main Streets alerts Anytown School District that the district's data has been hijacked, stating, "I'm the only one with the key. Pay me $2 million, and I'll provide a password so you can retrieve your data in time to make payroll tomorrow."

Anytown School District has 1,000 employees, which means 1,000 social security numbers, 1,000 home addresses and phone numbers, 1,000 bank account numbers, 1,000 routing numbers, and 1,000 email addresses, all stored in the district's computer system, are now inaccessible.

Anytown School District has fallen victim to a cyberattack.

A breach like this is more common than you might think, given the ever-growing sophistication of the cyber underworld. Ransomware attacks cost education institutions more than $53 billion in downtime between 2018 and 2023; U.S. schools alone lost an estimated $35.1 billion, according to Comparitech.

The District Leader Perspective

The *2024 State of EdTech Leadership* report, an annual survey administered by the Consortium of School Networking (CoSN) in partnership with AASA, The Superintendents Association, indicates that cybersecurity remains a top concern for edtech leaders, with 99% of districts taking measures to improve data protection. The survey of 980 edtech leaders from across the United States reported that an increasing number of districts are on a path toward implementing cybersecurity best practices.

How are districts responding to this urgent call to protect district data? Superintendents Mark Benigni, Peter Aiken, and Gustavo Balderas, and assistant superintendent of finance John Brucato provide their perspectives.

What is your district's overall approach to cybersecurity?

Mark Benigni, Meriden (Conn.) Public Schools: We try to build that culture of trust with our families. We do everything we can to protect student data and prevent data breaches. However, we also recognize that there are malicious actors out there who want to take advantage of school systems just like they're trying to take advantage of individual families and businesses.

How you react to the situation also lends to your credibility and your reputation.

Recently, we received an Education Security Preparedness Grant from IBM to help our schools prepare for and respond to the growing number of cyberattacks.

John Brucato, Briarcliff Manor (N.Y.) Unified Free School District: Our district has strict policies in place to protect our students and staff from cybersecurity threats. Our IT team is constantly monitoring our infrastructure and traffic to ensure any breaches or loss of important information are minimized. All employees must undergo annual cybersecurity training with information on the latest trends and threats made available.

Peter Aiken, Central York (Pa.) School District: Once you have that data breach or you have that hack, then you go into reactive mode. There's nothing that frustrates the public more than to say "Hey, we want more information" when we can't provide it. I think that's where that keen emphasis comes in: How can we be proactive in making sure that we're communicating in front of all this and really providing professional development ahead of all this?

Gustavo Balderas, Beaverton (Ore.) School District: It's a level of trust with your community and all stakeholders. It's how we react after and how we communicate to our stakeholders, our kids, our faculty, our parents, our broader community, and the local media.

How you react to the situation also lends to your credibility and your reputation. It's about making sure you react quickly with all the information that you can share and be resolved right afterward in terms of what you're going to do to deter it in the future.

Scaled-Up Cyber Awareness

Cyber criminals are more organized than we think and will go where they find success, which is why the education space continues to be a target. According to the U.S. Government Accountability Office, 647,000 American students were affected by ransomware attacks on K–12 schools in 2021. This explains why a robust cybersecurity defense plan is as important to a school district as any other crisis plan.

If your school district is lagging in this area and using outdated technology to protect internal systems, implementing a robust cybersecurity plan would be a substantial lift and investment, which means having that crucial conversation to prioritize adequate funds to upgrade protocols.

How do your bring cyber awareness to everyone in your district?

Brucato: In our district, all staff must participate in annual trainings. Throughout the year, our IT staff members generate random phishing emails that are sent to staff in order to simulate a real-world scam attempt. All staff members are able to report potential threats through an automated system and are encouraged to do so any time an email seems suspect.

Benigni: It starts with education and students. Part of the process could be having staff complete cybersecurity training as part of the annual training requirements. We do it as part of onboarding new staff members. We have our IT department share best practice emails throughout the district. All students receive digital citizenship and online safety instruction.

Aiken: I continue to stress professional development. The past two districts I served in worked with an outside agency. If we had somebody continue to click that "dancing monkey," we specifically worked with that individual. I think the vast majority of our staff appreciate that. It's in their face now and they get it.

Balderas: For us, it's making sure people understand our cybersecurity practices, from kids to families to staff, and making sure we're responsible for the information that we gather from our kids and our families and we keep it at a high level. We are constantly communicating to our staff and families regarding what we are doing. It's a constant training that we need to stay in front of.

Bottom line: A district may wish to bring in cybersecurity experts to examine what is already being done and to provide an objective, top-to-bottom view of the capability of systems to determine where the school system is as an organization and how it's protecting data and students against external threats.

Locking Down

You might say "We already have a robust system" or "We already have the necessary infrastructure." But

HELPFUL RESOURCES

The authors recommend the following resources.

- Webinar: Proactive Leadership Regarding Cybersecurity in School Systems, presented by CoSN and AASA. https://home.edweb.net/webinar/supers20240108/
- 2024 State of EdTech District Leadership Survey, published by CoSN in partnership with AASA. www.cosn.org/stateofedtech2024
- Back to School Safely: Cybersecurity For K-12 Schools/Fact Sheet published by AASA. http://tinyurl.com/AASACybersecurity
- February 2024 issue of AASA's *School Administrator*: Playing Defense Against Cyberattacks. https://www.aasa.org/publications/publication/february-2024-school-administrator
- CoSN/Cybersecurity Resources. https://www.cosn.org/edtech-topics/cybersecurity/
- AASA Cybersecurity Resources: aasa.org/cybersecurity
- The AASA Student & Child Privacy Center. https://www.aasa.org/resources/student-child-privacy-center
- ASBO International's Best of School Business Affairs Magazine "Cybersecurity Edition"
- ASBO International & CoSN Toolkit: Working Together For Student Success: A Guide for SBOs & CTOs
- Webinars from the ASBO International 2023 Annual Conference & Exp, available at https://learn.asbointl.org.
  - Creating Safer Learning Environments to Protect the K-12 Community https://learn.asbointl.org/topclass/topclass.do?expand-OfferingDetails-Offeringid=433646
  - Cyber Attacks Are Increasing https://learn.asbointl.org/topclass/topclass.do?expand-OfferingDetails-Offeringid=437110
  - Cybersecurity and Your School: Dealing with Vendors https://learn.asbointl.org/topclass/topclass.do?expand-OfferingDetails-Offeringid=437849

what are you doing to improve year after year? From an operations perspective, because everything runs off the network—security systems, cameras, locks, HVAC systems, bus schedules, cafeteria plans—those are some of the areas an attacker can manipulate to make your systems vulnerable, compromising the essential operations of a school.

Some attackers may masquerade as legitimate sources, spoofing themselves as employees or perhaps as concerned vendors offering to help a district mitigate the exact threats they're imposing. Students themselves might initiate the risk.

You can't implement best practices without sharing the context— the "why."

Many districts use a two-pronged authentication method, going beyond passwords and using a text message to verify who is attempting to log in. Some employees may see the added security as an inconvenience, which is why building a culture around the importance of data security is critical. You can't implement best practices without sharing the context— the "why."

How do you improve your existing systems/protocols year after year?

Balderas: We have multifactor authentication for our kids to make sure that it's not just the old one click—instead, it's two or three clicks. I know people don't like that, but it keeps us safe. It's not an end-all-be-all, but it helps us and it ensures people know we have everything possible in our systems to protect student data.

Benigni: It's education of staff and students for sure. We had a student take advantage of an unlocked teacher gradebook and significantly improve their grades. We want to look at how we time out those gradebooks, making sure that teachers are protecting that valuable data, and how we work with our students, too.

We also have done our own phishing campaigns to heighten awareness for staff and see who's clicking on that link that maybe they shouldn't click on. We can reinforce our own practices to keep everyone safe and protected.

Brucato: Our IT staff keeps up to date on the latest cybersecurity tends, threats, and best practices. We meet with the IT staff regularly to review policies and procedures and make necessary modifications to our practices to ensure compliance.

Aiken: The other one that we wrestle with now, too, is making sure our outside vendors bring that same level of security and appreciation for security that we're obviously trying to enhance here. There is no sense in us trying to lock things down airtight if some of these vendors aren't operating with the same set of rules.

Bottom line: Effective cybersecurity goes well beyond the efforts of the tech team. Many districts cannot afford a dedicated employee to focus solely on cybersecurity, so everyone must play a part. Some districts, such as

Beaverton School District, work with external partners, including local law enforcement and the local FBI office.

Communicating, Understanding, and Respecting the "Why"

We must work together to better understand the risks of leaving our systems and our data unprotected as cyber criminals continue hammering away at our systems. We cannot shy away from this critical issue. It will become more complex as the sophistication of the attacks escalates.

How do you communicate the importance of cyber awareness and emphasize why it's important?

Benigni: Keeping student information safe needs to be priority one—that's part of the balancing act—and then giving access as appropriate and asking those questions: Why do you need access? How can we monitor users who have access?

Aiken: The training piece is critical not only for staff but students as well. The more available we make ourselves and the better we are at communicating the why behind it all, the better.

Balderas: When working with educators, we need to ensure they understand the why behind these protective filters, why we have these rules of engagement. They need to know that it's to protect them and the students.

Brucato: School districts maintain a lot of sensitive information which can be a primary target for attackers. The SBO and administrative team need to be in regular communication with their IT department and have an appreciation for all of the time it takes to mitigate threats on a daily basis.

Do not underinvest in your technology and technology staff. Whether it's state of the art hardware, software or professional development, make budget allocations to stay ahead of any emerging threat. It's also worth considering an IT auditor to review your operations and make recommendations for improvement.

Bottom line: It's important to take stock of where you are. Not knowing the robustness of your cybersecurity system will leave your district rudderless. However, having a path toward improvement should be at the top of every district's priority list.

Keith Krueger is the executive director of the Consortium for School Network (CoSN). Email: keith@cosn.org

James Rowan is the executive director of the Association of School Business Officials, International (ASBO). Email: jrowan@asbointl.org

David Schuler is the executive director of AASA, The School Superintendents Association. Email: dschuler@aasa.org