Case Study

5 minutes with an edtech leader

How Lewisville Independent School District uses technology to build a safer school environment

Spanning more than 120 square miles in suburban Dallas–Fort Worth, Texas, the Lewisville Independent School District (ISD) is the 18th largest school district in Texas and 86th largest in the U.S.

More than 50,000 students attend the district's five high schools, 15 middle schools, and 40 elementary schools, where educators and staff are committed to educational success through real innovation and limitless opportunities for all students. Technology plays a vital role in enhancing education and the educational experience—including in ways that help ensure that everyone in the school community feels safe on campus.

Chris Langford, Director of Network, Infrastructure, and Cybersecurity at Lewisville ISD, shares how the district has deployed technology to ensure greater cybersecurity and physical safety.

What steps have you taken at Lewisville ISD to protect students, educators, and staff from cyber threats?

At Lewisville ISD, we balance investments in hardware, software, and services with education and training to protect our users. We've implemented a comprehensive suite of security solutions, from firewalls to malware protection (for endpoints and networks), email security, cloud security, network security, security analytics systems, content filtering, and more. With this technology, we're able to detect and stop threats, improve visibility so we know who is on our network, protect the privacy of our users and their data, and ensure compliance with regulations like the Children's Internet Protection Act.

Product List

- Cisco Firepower Next-Generation Firewall with Intrusion Prevention
- Cisco Advanced Malware Protection (AMP) for Networks and Endpoints
- Cisco Umbrella Security
- Cisco Identity Services Engine (ISE)
- Cisco Stealthwatch
- Cisco Cloud Email Security
- Cisco CloudLock
- Cisco Security Connector
- Cisco VoIP Phones
- Singlewire InformaCast

© 2019 Cisco and/or its affiliates. All rights reserved.

5 minutes with an edtech leader

Case Study

At the start of this school year, we implemented a mandatory cybersecurity training program for all Lewisville ISD staff. Then, throughout the school year, we conducted random phishing security tests; we alert staff members when they fall victim to a test phishing email, and we offer additional training to any who click too often.

Our students in fourth, fifth, and seventh grades participate in the Texas Digital Citizenship curriculum, which teaches them how to use technology responsibly and appropriately. They learn about things like protecting their privacy online, recognizing possible cybersecurity threats, and ways to address cyber bullying.

The results?

We use BitSight to help us measure the effectiveness of our efforts to keep users safe online, and we've improved our BitSight Security Rating by 70 points in eight months. (Note: BitSight uses an approach like credit score monitoring to assess an organization's cyber risk.)

We've also seen changes in the numbers of staff members who click on phishing security tests. Data from the service we use shows our results and tells us how we compare to other organizations. We decreased the click rate to our simulated phishing tests by more than 50 percent in less than six months.

How are you leveraging the network to ensure physical safety on campus?

In May 2017, the Lewisville ISD community passed a $730M school bond package, which included approximately $100M designated for technology. As a result, we've made investments in technology to address cybersecurity (including many of the solutions and training I mentioned above) and physical security over the last 18 months.

While we've implemented new technology to improve cybersecurity, we've also been able to increase our physical security posture, deploying upgraded security cameras in schools across the district. We're also in the process of upgrading our access-control systems and recently completed a VoIP phone system implemetnation at 53 locations.

We rely on an emergency notification system, which alerts administrators, school resource officers, school nurses, and other appropriate school or community personnel via text and/or email in the event of a tornado, lockdown, medical incident, or other emergency. Later this year, once all access control systems are upgraded, we'll integrate this system with our access-control, phone, and public-address systems so that alerts can be automated and issued by pressing just one button.

All physical security technology—like the security cameras and access-control systems—operate using the district network. Since implementation of the security technology coincided with an upgrade to our Cisco wireless network, we were able to integrate the security cameras easily into existing network ports. I'm confident that even if the implementations hadn't coincided, our existing network would be able to support technology improvements to enhance physical security. (Note: Lewisville ISD used funding from E-rate to help finance its wireless network upgrade.)

Learn more about how Lewisville ISD improved cybersecurity or discover more about Cisco's solutions for education.