4 Keys to Success with Zero Trust

These strategies will help K–12 schools navigate the zero trust journey.

WHILE ZERO TRUST CAN BE CHALLENGING TO implement, its potential for reducing risks and improving network security is significant. Here are four keys to success when moving ahead with a zero-trust approach.

1: Focus on change management.

When embarking on any large-scale IT initiative, school districts sometimes focus too much on the technology and not enough on the people and processes behind it. Taking a human-centered approach will greatly increase the likelihood of success.

To ensure a smooth transition, IT staff should anticipate the impact that zero trust might have on various school district operations and should plan accordingly. For instance, a business department that is processing payments might be sensitive to changes that could create problems for users.

"Zero trust is as much a cultural innovation as a technological one," consulting firm Deloitte **observes**. "Getting people to change their behavior requires communication and training." School district IT departments should lead a training and awareness campaign before

Not only are network users coming and going all the time, but their roles within the district frequently change as well.

implementing zero trust, so students, employees, and other stakeholders understand the purpose of this approach, how zero trust works, and where to get help if they encounter any problems.

2: Have good inventory control.

For zero trust to work well, "you have to get rid of applications that provide implicit trust," says IT consultant Joel Snyder, "or you have to segment them off from the other parts of your network." This requires having good visibility into the applications running on your network and a system for cataloging what these applications are and what ports they're using.

3: Keep user profiles up to date.

Under a zero-trust approach, permission to access data and resources is granted based on factors such as a user's role at the institution. This can be challenging to manage, especially within a K–12 setting — where student turnover happens every year and substitute teachers and volunteers frequently come and go.

Not only are network users coming and going all the time, but their roles within the district frequently change as well. These changes might require updates to their network permissions.

"Identity management can be an incredibly laborious and tedious process," says Doug Levin, national director for K12 SIX. "It involves close coordination with human resources departments." For zero trust to work effectively, school districts will need to invest sufficient time and resources in keeping user profiles up to date.

4: Make sure vendors are on board.

K–12 districts have transitioned to more cloud-based software in recent years, and IT leaders must make sure the cloud services they're using support a zero-trust model.

"All of your software-as-a-service vendors have to be on board with whatever you're doing for zero trust," Snyder says. "If a vendor is not going to be participating in the central authentication store you're using for identity and access management, then you've got a problem."

Snyder says he's working with a school district that's using a cloud-based administrative system from a small service provider. "I can tell from talking to the vendor that they don't really care about security," he notes. "Having your SaaS vendors and your IT department on the same page and at the same level of concern about security is critical."