K-12TechDecisions

Deep Dive:

Protecting Student Data

Personal devices are continuing to make their way into the classroom and that isn't likely to change. In fact, more schools than ever are choosing to go BYOD or to allow students and teachers to use mobile devices like tablets and laptops on school grounds. While these devices offer a myriad of learning opportunities, they also present a very real threat to your network. This article takes a look at how you can protect your network and mitigate the risks to student data.

Protecting Student Data

Personal devices are still the biggest threat, but there are steps you can take to mitigate your risks. *by Crystal Bedell*

LIKE EVERY OTHER ORGANIZATION operating in today's online world, K-12 school districts are faced with protecting sensitive data and granting access to that data via an increasing number of devices. But the more things change, the more they stay the same. Because even as sensitive student data is increasingly stored in the cloud, the risk remains largely the same: the unmanaged endpoint.

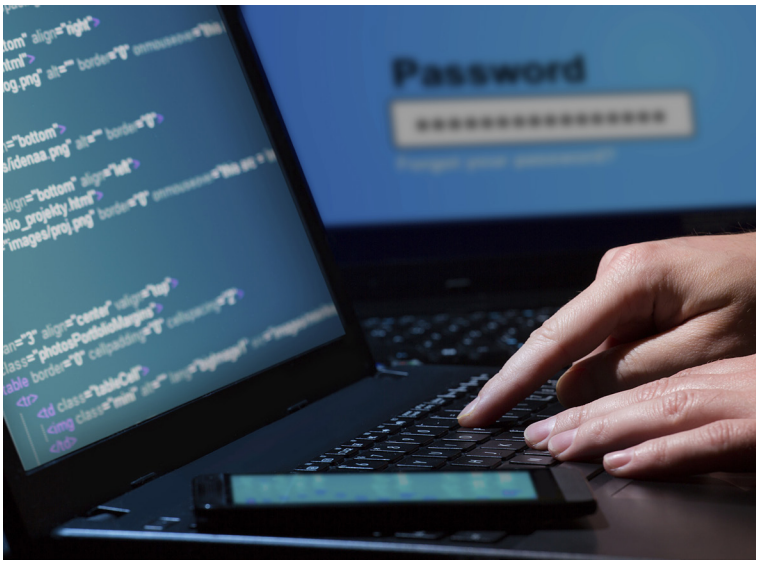
"A lot of school districts are doing away with locally housing any student information . . . two-to-three years ago the average district had 30 servers. That's been cut in half – if not more – simply by this movement," says Joddey Hicks, northern sales manager for Heartland Technology Solutions, an IT solution provider based in the Midwest.

Increasingly, education software providers are hosting their applications in their own data centers, or the cloud. Users access these applications, like student records management systems, via a Web browser or mobile device. According to Ben Sylvester, director of IT services for K-12 Technology Group, a Menomonee Falls, Wisc.-based managed services provider, the risk to student data in this case "depends on the quality of the internal management of the devices used to access the student records management system [in the cloud]."

Sylvester says education software providers use the same technology to protect student data – SSL – that financial services organizations use to protect financial data online. SSL is fairly reliable, and most providers use best practices to secure data. "As far as a web connection, that's difficult to hack, but hacking access to the system being used [to access student data] can take place at a lower level," he says. "User systems aren't being secured adequately to provide the password security that is, in the end, the most critical piece for accessing the information."

Sadik Al-Abdulla, director of security solutions for CDW, a Vernon Hills, Ill.-based IT product and service provider, agrees. “If you have a cloud service – a transcript and grading service – they have phenomenal security. They are doing everything right. The weak point is the credentials – how you log on to that system.”

If users access student records using a simple text-only password that is not renewed on a regular basis and it gets hijacked via a vulnerability on the underlying system, then an attacker can use any device to login as the user and access student data, explains Sylvester. And that leads us to what Sylvester and others say is the greatest threat to student privacy: poor systems management.



“Ultimately, on almost any workstation, vulnerabilities will be exposed over time. The providers release security updates, and the end user has a responsibility to react to that release,” says Sylvester. “If you don’t have consistent management of the system and apps used on the device, inevitably that vulnerability could be exposed to the wrong people.”

Hicks says this is a particular problem when district IT departments are provisioning and managing a mobile device for each student in a 1:1 program, as well as staff and administrators. “[Microsoft users] are the ones that usually get missed the most because moving to a 1:1 you’re so focused on the mass population, you forget about your power users. You think Microsoft users are updated, but they haven’t been for months because users are in the middle of something and click to postpone an update and don’t get back to it,” he says.

IT also has its hands full. “There’s almost a status quo hands-off-like approach in terms of workstation management. There are responsibilities and a level of work that overwhelms staff members in school districts to the point that they have to prioritize what gets done, and the ‘if-it-ain’t-broke’ strategy creates too much latency in managing systems that handle sensitive information. Security fixes need to be deployed in real time when they are published, and most districts don’t have a mechanism to handle that,” Sylvester says.

To make matters worse, experts say that some districts are still running Windows XP – for which there are no security fixes. Microsoft discontinued support for the operating system (OS) in April, so any vulnerabilities discovered in the OS will remain exposed as long as it's running. "[XP] is no longer being supported and is considered insecure, but because of budget considerations it still exists in too many districts," Sylvester says.

According to Hicks, the school districts he works with knew that XP was end of life, but they didn't know the extent to which it would affect them. He explains that most of the applications are Web-based so schools can't update things like Internet Explorer or Chrome on XP. "Suddenly everything comes to a head at once. [Districts] thought they could squeak through for a couple years. Microsoft has never been this adamant about killing an OS. People thought they'd call them on their bluff, but MS needed to do it because of security issues and other stuff," Hicks says.

If school districts lack the resources to properly manage desktop workstations, then mobility and bring your own device (BYOD) programs only exacerbate the problem. "BYOD is the biggest concern where staff members are bringing their own computers in and accessing student records. I have a lot of control over district owned devices. There's a loss of control with staff-owned BYOD scenarios," says Sylvester.

He continues: "The updates become a gray area and a potentially significant problem. There has to be, in my opinion, a strategy that outlines similar management methods to cover [personally owned] devices that parallels the internal devices – and you must have the budget to support it. You're scaling the labor and software costs significantly, and making it unaffordable to manage it. BYOD – bring your own device to access our resources – brings with it the overhead associated with poor management of that device."

How to protect sensitive student information

With the risk to student data resting on poor systems management, advice for protecting that data focuses on getting back to the basics. "[School districts should] be very focused and disciplined in their management of devices being used to access their student records information and finance system," says Sylvester. "That means being absolutely certain that all devices have adequate protection in terms of malware and antivirus, using certified applications that aren't chosen based on budget, but are based on quality for any devices that are accessing sensitive information. That means utterly eliminating XP from the equation. No one should use it to access student information."

Sylvester also recommends having a verification process to ensure that updates have been installed. "Oftentimes the update process for antivirus is interrupted through an installation failure or software corruption, and the end user isn't aware of the fact that the antivirus is not being updated."

When it comes to securing mobile environments, Al-Abdulla says three things need to be considered: the network, the data and the devices. "When you create an environment that enables mobility and wireless access to sensitive systems, the network itself can be an attack point," he says. "Oftentimes, wireless networks grow up organically, and in the process of scaling, people don't allocate the proper attention to securing the network."

The data should be protected through encryption, and as a baseline, the devices should be protected via a mobile device management (MDM) system. Al-Abdulla said MDM systems allow organizations to set policies requiring users, for example, to turn on encryption functionality, the screen lock, and certain types of authentication to access particular systems. MDM systems also give organizations the ability to do a remote wipe of a system if it becomes lost or stolen.

"I wouldn't say those things protect you entirely, but those are the things that have to be done, "Al-Abdulla says. "These are still personal devices that people can have the majority of control over, but making sure they are up to date, encryption is turned on and that if they are stolen, you can wipe them, is critical." ■