Blazing a Mobile Trail: Four Things Districts Must Consider for BYOD

For a BYOD policy to be successful, a healthy amount of preparation is in order.

By Chris LaPoint

In the 1980s, many students learned about a key period in U.S. history, not through textbooks but on a computer screen. Their tutor was, of all things, a video game called *The Oregon Trail*. Students assumed the role of a pioneer family making its way from Missouri to Oregon. They learned about the harsh realities of life in the 1800s, including proper ways to hunt, the threat of diseases, and more. It was one of the first examples of using modern technology to engage and teach in different, exciting, and even fun ways.

The Oregon Trail game still exists today, but in a much different format. Today's students can download it to their iPhones and iPads and can experience the thrill of the Old West just about anywhere—including in their classrooms.

Given the popularity of mobile devices among today's students, it looks like many of them want to have the option to do just that. According to a recent survey conducted by the education services company Pearson (2013), 69% of elementary, middle, and high school

students would like to use mobile devices more often in the classroom. That survey also found that many students already own their own mobile devices and would appreciate using them for schoolwork if their schools would allow them.

And more schools *are* allowing them. Following the U.S. Department of Education's 2010 National Education Technology Plan, which outlines how the current "bring your own device" (BYOD) trend could help enhance education, more school districts have begun to—to use a phrase that might be found in *The Oregon Trail*—"cotton to" the use of smartphones and tablets. If you combine that interest in technology with U.S. Secretary of Education Arne Duncan remarks at the 2012 South by Southwest conference—in which he said that technology was providing students with "access to more information through a cell phone than [he] could find as a child in an entire library"—you will have a school system that not only has become accepting of mobile devices, but welcomes them.

Measures for Success

No one doubts that having access to information at the touch of a finger (and yes, to *Angry Birds*—but let's not go there) has potentially significant educational benefits, but having so many personal mobile devices on school networks has given information technology (IT) managers reason for pause. That's because such proliferation also introduces significant new concerns and risks to school networks, including fears regarding security, the use of bandwidth, and more.

All of that wonderful information that's being delivered uses a lot of bandwidth.

Therefore, for a BYOD policy to be successful, a healthy amount of preparation must be done to ready the school's infrastructure for handling the influx of mobile devices within classrooms and corridors. Specifically, four measures need special consideration in order to keep school networks from crumbling under the weight of the mobile influx.

1. Monitoring Networks and Devices

Whereas *The Oregon Trail* once introduced kids to the Wild West, smartphones and tablets are threatening to create their own version of that unruly place in today's schools. With personal devices coming from everywhere, it can be challenging for IT administrators to keep track of who is accessing their networks, what data are being shared, and when. But doing so is absolutely essential.

Likewise, school IT administrators should have a network monitoring system in place that automatically alerts them to potential trouble on the network, including outages, downtime, and other factors. Ideally, they're already doing that; if they're not, the growing number of mobile devices that will soon be using their networks will make it a necessity. All of those devices operating on the network can substantially raise the risks of less-than-ideal network performance; administrators will want automated tools that help mitigate that problem.

2. Watching Access Points Closely

As the number of mobile devices on school networks increases, so does the number of switches, ports, and Wi-Fi access points that administrators need to monitor. Such monitoring is important as IT managers look to get a grasp of what devices are accessing their networks and who's using them.

As such, careful monitoring of access points can provide a great deal of useful information. That information includes where users are connecting to the network, historical data on individual devices that have connected (and the students and faculty using them), the types of devices being used, switch capacity, and more. Perhaps even more important, monitoring can provide managers with vital information to better plan for checking for rogue, potentially threatening devices and managing bandwidth.

3. Tracking Rogue and Suspicious Devices

Today's schools house not only academic information but a wealth of data that many hackers would love to get their hands on, including personal information about students and faculty members. With so many new devices being brought into schools, it could be difficult to determine which ones are innocuous and which might be trying to access the network to get the principal's home address.

Fortunately, administrators who are taking Measures 1 and 2 are already in pretty good shape for blocking those devices, or at least tracking them down. The information gleaned from IP addresses and access points can be used effectively to mitigate potential threats from unauthorized devices that may be trying to access data. If there's even a hint of a security breach, administrators can quickly search for a particular device by using the IP address, media access control address, or hostname. Once the suspicious device has been located, managers can determine the switch or port to which it was connected and then shut down that port.

Unfortunately, that procedure can be very time-consuming, especially as more devices are brought into the school. It can be difficult for network administrators to keep track of every smartphone, laptop, or tablet that is connecting to the network, making it tough to discover who or what may be using that network for nefarious purposes. Are they stolen devices? Are students using

those tools for unauthorized—even illegal—purposes? Those are the practical concerns that really compound the issue of BYOD monitoring.

Thankfully, IT managers can use a couple of strategies to identify those devices and prevent other unauthorized devices from gaining network access.

Through UDT, the system can automatically map and monitor switches, ports, and network devices.

First, managers can develop a "watch list" of potentially suspicious devices and have network monitoring systems send alerts when those devices are attempting to access the network. The system can automatically scan for those devices and help avert a potential security breach.

Second, they might consider implementing user device tracking (UDT) software. Through UDT, the system can automatically map and monitor switches, ports, and network devices. UDT also provides a means for administrators to quickly identify and track the location of a particular user, right down to his or her seat in a classroom or the library.

4. Watching Bandwidth Consumption

It's not like administrators need any *additional* devices on their networks—they're already going to have plenty of authorized ones to deal with. That means barely enough bandwidth for all staff and students.

The ability of tablets and smartphones to deliver streaming media, web access, apps, and more has made them exceedingly useful in the classroom. But all of that wonderful information that's being delivered uses a lot of bandwidth, the consumption of which is going to inevitably increase.

Thankfully, bandwidth consumption doesn't have to get out of hand, and administrators can take several approaches to control it. First, they can set up specific security privileges for the volume of data that certain individuals can consume. An example would be allowing teachers to have greater bandwidth privileges than students by logging into the network via their own portal or credentials. Managers may also implement a network bandwidth monitoring system that will automatically alert them to excessive bandwidth usage. Such a system can help managers gauge how much data are passing through their network through the mobile devices, even down to the specific user, at which point they can learn which devices are using the most bandwidth, at what times, and by whom, so they may plan accordingly.

Preparing for the Journey

Although today's world of portable devices may seem like the lawless land those poor souls from *The Oregon Trail* had to deal with, it doesn't have to be. Like today's students, those pioneers excelled through wits, knowledge, and focus. They're the same attributes that IT administrators can use to arm themselves against the BYOD invasion. The more they know about what's going on as a result of those devices, the better equipped they'll be to handle any potential mishaps.

Reference

Pearson. 2013. New study reveals U.S. students believe strongly that mobile devices will improve education. www.pearsoned.com/new-study-reveals-u-s-students-believe-strongly-that-mobile-devices-will-improve-education/#.UwDZWPldVI6.

Chris LaPoint is vice president of product management at SolarWinds, an IT management software provider based in Austin, Texas.

Index of Advertisers