VIPRE AntivirusBusiness

Does Your School's Mobile Security Make the Grade?

Mobile Devices Take Over Campus

The days of preventing mobile device use during the school day are history. The new reality is tech-savvy kids and teachers alike are using personal and school-issued smartphones and tablets in classroom activities, and it is forcing IT administrators in K-12 education to address a growing concern.

While iPads, iPhones, Android devices and e-Readers are enhancing the learning experience, they may also be posing risks to a school's network security at the same time. No longer is Bring Your Own Device (BYOD) a phenomenon unique to the business world – nor is the corresponding need for a comprehensive Mobile Device Management (MDM) solution.

Schools are encouraged to adopt BYOD initiatives as part of the U.S. Department of Education's 2010 National Education Technology Plan (NETP). Yet BYOD in education raises various red flags. Chief among them are concerns regarding data protection, compliance with the Children's Internet Protection Act (CIPA) and, perhaps most critical in today's K-12 world, the potential for introducing malicious software with the capability to sabotage a school's network.

"Being the first school in the area to allow students to bring their own devices may help a school sound progressive and current. However, if they do not have the proper infrastructure and are not prepared for the change of culture that this can have, the schools only look good on paper," Peter DeWitt, an elementary school principal in Albany, N.Y., wrote for Education Week.[1]

Incorporating technology into K-12 studies is hardly a new practice. PCs for years have carved out a place in the classroom.

But PCs struggle where mobile devices – tablets, in particular – are flourishing. Mobile devices provide students with collaborative access to classroom resources, creating an atmosphere for around-the-clock learning. Teachers, in turn, can incorporate the various devices into

Bring Your Own Device (BYOD) is no longer a phenomenon unique to the business world – nor is the corresponding need for a comprehensive Mobile Device Management (MDM) solution.

The widespread use of mobile devices that access school networks has created new IT security headaches. Many of the devices that connect to a school's network have minimal antivirus protection, if any at all, introducing new risks that must be addressed.

their lesson plans, work with current digital textbooks rather than outdated print editions and foster a culture of one-to-one learning that extends beyond classroom walls.

By many accounts, Apple has made the most significant inroads in K-12 education. A recent study entitled "Kid Tech According To Apple"[2] found that 1.5 million iPads are currently used by U.S. students and more than 20,000 education applications are available for the device.

The study also found that the percentage of digital textbooks on the market doubled from 3% in 2011 to 6% in 2012. The percentage is estimated to surpass 50% by 2020.

"I would say an iPad will one day be the same as a book bag or a ruler or a pencil. I think that the iPad will be an essential component to schools, (and) it's certainly something we can't ignore as a school – we need to embrace it," Michael Singleton, the social studies department head at Florida's Orlando Science Schools, told U.S. News.[3]

51% of K-12 IT admins said securing mobile devices was their top concern.

However, the widespread use of mobile devices that access school networks has created more IT headaches related to malware threats than data protection. Many of the devices that connect to a school's network have minimal antivirus protection, if any at all, creating vulnerabilities on school machines when the network is accessed.

Research shows IT security in K-12 schools is good in some areas. But there is little question that, in other areas, it needs to be better.

IT Admins Could use a Boost in Confidence

A study by GFI Software found that the majority of IT administrators from public (71%) and private (28%) U.S. K-12 schools believe they are achieving a suitable level of network security on school-owned and school-managed systems. In fact, 91% of respondents rated their general IT security readiness as "good" (adequate solution) or "strong" (comprehensive solution).

But a deeper look into those findings presents a noteworthy revelation: IT administrators at K-12 schools are confident in their IT security readiness when it comes to areas where they have some level of control and access to relatively mature technologies that assist them in management practices.

Respondents rated their IT security readiness as "good" or "strong" in four categories. The categories were:

- Email security (96%)
- Malware prevention (94%)
- Data privacy (94%)
- Web monitoring (91%)

By contrast, the two categories where respondents rated their confidence in IT security readiness as "poor" or "don't know" were:

- Securing personal devices accessing the school network (27%)
- End user network security education (21%)

In these areas, the reason network administrators lack confidence is they have less control. Educating mobile device users on network security isn't enough. And while securing personal devices that access a school's network can be addressed by technology, doing so is often costly and difficult to administer and manage.

Not surprisingly, these security concerns that stem from IT administrators having less control are increasing at the fastest rate.

GFI's study showed that 51% of respondents cited their top concern as securing mobile devices that access the school network. Just two years ago, 18% of IT administrators considered the issue their top challenge.

Mobile-Targeted Malware is on the Rise

When contemplating which of the many threats to their network is highest priority, small- and medium-sized businesses (SMBs) typically start with ensuring sensitive material remains safe. Unlike SMBs, however, K-12 schools largely believe their data is secure and therefore view malware as more harmful to their operation, according to GFI research.

With the vast number of students and faculty accessing a school's network via personal or school-issued mobile device, IT administrators identified the clear-cut top security pain points.

Atop the list is the lack of adequate antivirus protection on the many devices that access the school network (40%). That concern goes hand-in-hand with the two other issues: students, faculty and employees accessing the network with mobile devices (38%) and the lack of in-house resources and personnel needed to provide suitable IT security (38%).

These findings further support the earlier point that a lack of control is the biggest hurdle IT administrators must clear. And the sooner they do it, the better. Risky behavior is commonplace, even if it is unintentional. Malware writers and cybercriminals know it, and they have adjusted their tactics to make mobile devices do their dirty work.

The Government Accountability Office (GAO) in September 2012 submitted to Congress a report on mobile device security. The report noted that mobile-targeted malicious software – viruses, spam and phishing attacks – has nearly tripled in the past year. It skyrocketed from 14,000 to 40,000.[4]

1.5 million iPads are used by U.S. students.[2]

The Need for MDM is 'Only Going to Grow'

The K-12 learning experience is clearly changing. More schools are seeing the value in issuing mobile devices to students, or allowing them to use their own for instructional purposes. This escalating trend proves that educators believe the benefits that mobile technologies provide outweigh the risks that come with their use. Or to K-12 IT admins' misfortune, teachers, staff, school boards, students and parents clamoring for mobile devices in the classroom are simply unaware there is any threat at all.

By no means should mobile threats be taken lightly. However, schools don't need to be afraid of enhancing how they educate because of potential risks – particularly when cost-effective network solutions exist for IT administrators to easily deploy and manage.

With the proper solution, IT administrators have complete control. They gain the ability to manage all devices accessing the school's network, ensuring optimal use of technology without compromising IT security.

Benefits of MDM include the ability for IT administrators to:

- Protect their networks against Android malware
- Remotely alarm, locate and wipe lost or stolen devices
- Manage Wi-Fi configurations on mobile devices
- Enforce passwords on iPhones and iPads
- Streamline operations
- Increase efficiency
- Focus on higher-priority IT tasks

"A key task for IT administrators is to secure and manage mobile devices, whether they are student- or district-owned, so users have a consistent and safe experience regardless of the device and (operating system)," reporter Carol Patton wrote for Scholastic.com.[5] "And … this discussion is happening in almost every district, and the need for MDM and mobile protection is only going to grow."

About VIPRE Business Premium

VIPRE Business Premium is the small-footprint antivirus software that enables IT administrators in K-12 schools to secure all devices that access their network with MDM for iPhones, iPads and Android smartphones and tablets, built-in Mac support, removable media scanning and unprotected computer identification.

In addition, VIPRE includes integrated patch management, a groundbreaking feature that automatically updates out-of-date software, eliminating the number one cause of PC infections and attacks: unpatched machines.

Visit **www.gfi.com/vipre** to evaluate VIPRE Business Premium free for 30 days.

[1]EducationWeek.com, Are Schools Prepared To Let Students BYOD?, August 2012
http://blogs.edweek.org/edweek/finding_common_ground/2012/08/are_schools_prepared_to_let_students_byod.html

[2] Apple, Kid Tech According To Apple, 2012
http://www.ipadinschools.com/wp-content/uploads/2012/09/kid-tech-infographic.jpg

[3] USNews.com, Tablets Trump Laptops In High School Classrooms, August 2012
http://www.usnews.com/education/high-schools/articles/2012/08/03/tablets-trump-laptops-in-high-school-classrooms

[4] NetworkWorld.com, The 10 Most Common Mobile Security Problems And How You Can Fight Them
http://www.networkworld.com/news/2012/091912-mobile-security-262581.html

[5] Scholastic.com, Mobile Impact, 2012
http://www.scholastic.com/browse/article.jsp?id=3757443