Does Your Campus Mobile Security Make the Grade?

Summary

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 and management headaches that administrators need to address now.

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

While iOS and Android devices enhance the learning experience, they expose institutions to new security risks at a time when educators are under increasing threat from cyber-attacks.

Since 2012, there have been 67 major education data breaches reported, impacting more than 2 million student and employee records[1]. And as mobile malware continues to rise, education IT departments at all levels need a solution to solve their Bring Your Own Device (BYOD) security and management issues.

2+ million
records compromised in education data breaches since 2012

Mobile Devices Take Over Campus

Incorporating the latest technology into studies is hardly a new practice for education IT professionals. They are always under pressure from government, school boards, administration, students, parents and even donors to continually modernize their technology, and to do so with tighter budgets and shrinking staff.

Where PCs have struggled, 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in turn, can incorporate the various devices into their lesson plans, work with current digital textbooks rather than outdated print editions and foster a culture of one-to-one learning that extends beyond classroom walls.

Clearly, mobile devices are here to stay. It's estimated that one-third of U.S. students now use school-issued mobile devices[2]. But unlike deploying a refreshed PC fleet, speeding up Internet access in dorm rooms or virtualizing servers to cut infrastructure costs, introducing mobile devices creates an entirely new attack vector that cannot be ignored.

The Wild West of Malware

Mobile malware is growing exponentially. In 2012, it was estimated that there were about 10,000 known malware threats attacking mobile devices. Now, ThreatTrack Security processes nearly 1,500 mobile malware threats every day.

Some security researchers claim that new mobile malware threats – broadly inclusive of the slightest variations – neared 2.5 million in 2013[3], and it is estimated that 99% of all mobile threats target Android devices[4].

The rise of mobile malware is reminiscent of the rapid growth of PC malware, as cybercriminals take advantage of users' naivety and unfamiliarity with the threats they face on these new devices. However, this time the cybercriminals have an even stronger advantage since they can call up more than a decade's worth of proven tricks and ploys compromising Windows machines to infect as many smartphones and tablets as they can.

We are seeing mobile malware unleashed for a wide variety of malicious purposes. Most commonly, mobile malware takes the form of malicious or rogue apps. These apps are developed to entice users to install them for the purposes of stealing data like passwords, running up text and voice charges, spamming users with unwanted ads and more. This tactic is unsurprisingly effective for cybercriminals as the main perceived benefit of mobile devices for users is the access to countless apps, and their desire to find, download and try the latest free games and entertainment services.

1,500+

mobile malware threats analyzed every day

Other forms of mobile threats include hijacking smartphones and tablets to create a global network of bitcoin mining bots via threats called BadLepricon and CoinKrypt[5]. Taking another page directly from the PC attack plan, cybercriminals are examining app code for vulnerabilities to be exploited, creating Zero-day threats for mobile users. Mobile threats also are starting to jump platforms, with malware traversing PCs – avoiding detection by antivirus looking for PC threats – to indirectly infect smartphones[6].

It doesn't matter whether your students, faculty or staff encounter these threats while using their devices for personal or work-related activities. As soon as those devices become infected and access your network, it becomes a problem for IT admins. How do you know what devices are infected? What infections may have been introduced to your environment? Without an MDM solution, you have no way of knowing.

Privacy and Data Loss

According to Consumer Reports, 3.1 million Americans had their smartphone stolen in 2013, and 1.4 million lost their smartphone over the same time period[7]. The report went on to illustrate how careless users are with their mobile security with 34% of those affected not taking any security precautions at all.

Of those who did, only:

- 36% set a screen lock with a 4-digit PIN
- 22% installed software to locate a lost phone
- 14% used an antivirus app
- 11% had a PIN longer than 4 digits or a unlock pattern

The data clearly reinforces that IT admins cannot leave mobile security in users' hands. Unsecured devices that can access district or university email and documents are a tremendous risk and liability. Not only is the personal information of students and staff left vulnerable, users unknowingly storing sensitive data on their smartphones may expose your institution to lawsuits, as well as fines for failing to comply with industry or government regulations.

IT Admins Need Boost in Confidence

A study by ThreatTrack Security 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:

- 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.

Higher education faces similar issues. A study by the University of Florida concluded that "mobile devices are proliferating and demand for mobile-enabled services is increasing. As a result, more institutions are launching mobile initiatives, and schools without them are experiencing pressure to do so."[8]

The study went on to explain that security remains a primary concern. Findings stated, "The services desired by users reflect everything from easy-to-implement 'low-hanging fruit' to more complex access profiles that implicate security issues (access/authorization) and privacy considerations (FERPA, HIPAA, PII) as well as protection of institutional revenue streams and intellectual property. Therefore, institutional mobile initiatives will need to engage policymakers, legal counsel, security experts, and others as well as IT and development shops when an institution 'goes mobile.'"

Limit Security Risk with MDM

Educators continue to discover the value of teaching with mobile devices. In lieu of school-issued devices, they will allow students to use their own smartphones and tablets in the classrooms. That leads to trouble.

Education IT professionals need to take charge by setting and enforcing appropriate BYOD policies and by implementing a comprehensive Mobile Device Management (MDM) solution across all school-issued devices.

For student- or staff-owned devices accessing any school assets, including email:

1. Establish minimum operating system requirements for Android and iOS devices
   a. Outlaw jailbroken phones
   b. Devices and installed Apps must be patched when updates are available
2. Mandate that users implement access passwords and screen locks
3. Require users install to security software to defend against mobile malware, help locate lost or stolen devices, or wipe lost devices
   a. Require users to alert IT to any lost or stolen devices immediately
4. Remind users that all data access, usage and storage guidelines apply to mobile devices
5. Do not allow personal devices not managed by IT to directly access the network
   a. Create a separate Wi-Fi network for unmanaged devices that complies with best practices for password strength

Of course, your policy is only good if users fully understand the consequences associated with failing to comply, and their track record – especially students – when it comes to security is nothing any IT admin wants to rely on 100%.

Consequently, the best course of action for any school or university serious about adopting mobile devices is to issue and manage the smartphones and tablets themselves. 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 the technology without compromising IT security.

Benefits of MDM include the ability for IT administrators to:

- Protect their networks against mobile malware
- Defend against data breaches
- Remotely locate and wipe lost or stolen devices
- Manage Wi-Fi configurations on mobile devices
- Enforce passwords strength requirements
- Manage all mobile devices centrally from a single console

VIPRE Antivirus Business and VIPRE Business Premium offer an integrated MDM feature set of robust defenses

against known and emerging mobile malware for Android devices. By installing the VIPRE MDM agent on all your mobile devices, you know they are secure and malware free, and you have control over scans, updates and more.

Moreover, VIPRE offers the ability to locate lost or stolen devices on a map for retrieval or to share with law enforcement, as well as to sound an alarm for lost Android devices, and remotely lock iOS devices. Thieves cannot uninstall the VIPRE MDM agent. Only the VIPRE administrator is authorized to uninstall agents, ensuring that sensitive data, passwords and network access does not fall into the hands of cybercriminals. VIPRE MDM also provides IT admins with the ability to set Wi-Fi passwords and enforce password strength standards on all managed iOS devices.

About VIPRE

VIPRE is ThreatTrack Security's small-footprint antivirus solution for businesses and organizations of all sizes, including enterprises, educational institutions and government agencies. Optimized to quickly scan for threats without slowing down PCs, VIPRE has been a preferred endpoint protection solution for IT security professionals for years. Both versions of VIPRE's enterprise solutions – VIPRE Antivirus Business and VIPRE Business Premium – offer integrated Mobile Device Management (MDM) with Android antivirus, and mobile security for iPads, iPhones and Android devices.

Secure and manage the mobile devices accessing your network. **Try VIPRE free for 30 days**.

About ThreatTrack Security Inc.

ThreatTrack Security specializes in helping organizations identify and stop Advanced Persistent Threats (APTs), targeted attacks and other sophisticated malware designed to evade the traditional cyber-defenses deployed by enterprises and government agencies around the world. The company develops advanced cybersecurity solutions that **Expose**, **Analyze** and **Eliminate** the latest malicious threats, including its ThreatSecure advanced threat detection and remediation platform, ThreatAnalyzer malware behavioral analysis sandbox, ThreatIQ real-time threat intelligence service, and VIPRE business antivirus endpoint protection.

1. Privacy Rights Clearinghouse; https://www.privacyrights.org/data-breach

2. The Journal, One-Third of U.S. Students Use School-Issued Mobile Devices, 2014; http://thejournal.com/articles/2014/04/08/a-third-of-secondary-students-use-school-issued-mobile-devices.aspx

3. ComputerWeekly.com, Dark web key enabler for cyber criminals, 2014; http://www.computerweekly.com/news/2240215842/Dark-web-key-enabler-for-cyber-criminals-say-researchers

4. ComputerWeekly.com, Cyber criminals continue to target Android smartphones, 2014; http://www.computerweekly.com/news/2240219722/Cyber-criminals-continue-to-target-UK-Android-smartphones

5. ThreatPost, Google Removes Bitcoin Mining Android Malware From Play, 2014; http://threatpost.com/google-removes-bitcoin-mining-android-malware-from-play/105740

6. Tech Target, Mobile security: The battle beyond malware, 2014; http://searchsecurity.techtarget.com/feature/Mobile-security-The-battle-beyond-malware

7. Consumer Reports, Smart phone thefts rose to 3.1 million last year, 2014; http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm

8. Educause Review Online, A State of Flux: Results of a Mobile Device Survey at the University of Florida, 2013; http://www.educause.edu/ero/article/state-flux-results-mobile-device-survey-university-florida

To learn more about ThreatTrack Security
call +1-855-885-5566 or visit www.ThreatTrackSecurity.com.

ThreatTrack SECURITY