EDTECH™ FOCUS ON HIGHER EDUCATION

Brought to you by:

CDW·G

CASE STUDIES

TACTICAL ADVICE

RESOURCES

Classroom

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management

CURRENT ISSUE

EDTECH
FOCUS ON HIGHER EDUCATION
High-Speed Learning
Washington's broadband network brings top-quality education to remote areas
24

Subscribe

2012 CAMPUS TECHNOLOGY
19th Annual Education Technology Conference
Read the latest reports from Campus Technology 2012 in Boston.
EDTECH

SIGN UP FOR

EdTECH

E-NEWSLETTERS

Follow EdTech

Follow RSS Feed

Connect With CDW

LinkedIn YouTube Spiceworks

Like 6.7k

Home » Security

‹ previous next ›

Bring Your Own Device (BYOD)

## BYOD Is a Big Deal on Campus

**Accepting students' mobile devices on campus networks requires IT shops to shore up security.**

Karen D. Schwartz

posted May 18, 2012 | Appears in the Spotlight on Network Security issue of the *EdTech Magazine* e-newsletter.

Like 0 Tweet 5 Share Spice

Related Articles

What Colleges Can Learn from Mat Honan's "Epic Hacking"

Building a Flexible BYOD Program

Firewall Rule Management Is the Key to Network Security

4 Strategies for Preventing a Data Breach

Review: Fortinet FortiGate–300C

Editors Picks

Three Easy Steps to BYOD

5 Tips for Optimizing Load Balancers
Why Computer Labs Are Still Essential On Campus
Higher Ed Scope

Types of schools featured: Public University

About a year ago, West Chester University of Pennsylvania created a formal policy to allow students and guests to use their own mobile devices on the campus network. The decision to implement a “bring your own device” (BYOD) program was made partially to coincide with a campus move to go fully wireless and partially to acknowledge that students had been using their own devices on campus for years anyway. That’s when the real work began.

Because students would no longer be accessing the network as guests but would be full-fledged users, security and management had to be iron-clad. West Chester implemented a system under which students enter the network through Microsoft Active Directory and are validated through *Aruba Networks’ AirWave*, a mobile-device management (MDM) solution that keeps track in real time of which devices and users are on the network, what they are accessing and how much bandwidth specific devices are consuming.

For guests — for example, users on campus for a conference — the IT staff installed *Aruba Networks’ Amigopod*, which provides secure wireless Internet access.

CIO Adel Barimani is considering implementing a third Aruba solution, AirGroup, which securely identifies users based on their roles (student, visiting professor, etc.) and location before allowing them access to network services, such as wireless printing.

“So far, the technologies are working really well,” Barimani says. “Our latest numbers show that we have an average of 8,000 unique wireless devices registered, with 2,200 concurrent users daily.”

Barimani realizes that accepting mobile devices onto the campus network requires the IT staff to strengthen network security. Without that, the IT department can quickly lose control of who is accessing data and applications and whether the devices they are using are fully secure, leaving the organization vulnerable to unauthorized access to sensitive information.

For organizations that let users save or download data to their mobile devices, the first step is to implement some type of mobile-device management solution. MDM monitors devices that are connected to the network and can remotely lock or wipe these devices.

Even if an organization doesn't let users download or save data on their personal devices, security is still a priority, says Andrew Braunberg, research director for enterprise networks and security at Current Analysis in Herndon, Va. Many solutions can bolster network security for BYOD. The goal of mobile application management (MAM) products is to make apps more manageable and secure. Some solutions accomplish this with "wrappers" that control the use of the application. Others use containerization, which creates private "sandboxes" for sensitive apps.

Hypervisors, which create virtualized platforms that ride on top of the operating system, and data loss prevention technology also help protect the network against the risks associated with personal devices.

BYOD is standard practice for the University of South Florida's 47,000 students, who access the school's open wireless network from a variety of devices. Students must register their devices each semester to use the network, which then authenticates the device's MAC address. The unencrypted open network uses a homegrown network access control (NAC) system for protection and can quarantine a device if it is found to have a virus or otherwise poses a security risk, says Senior Network Engineer Joe Rogers.

**61%**
The percentage of organizations that allow users to access network resources via personal devices.

**SOURCE:** SANS Mobility/BYOD Security Survey, March 2012

The university has a second, more secure network as well, which students can use if they need they need public IP addresses (the open network uses private IP addresses and limits some applications that don't deal well with network address translation).

Both networks use an intrusion detection system that combines analysis and log monitoring tools based on NetFlow, a protocol developed by Cisco Systems to collect IP traffic information, along with *Tenable Network Security's Nessus* vulnerability and configuration assessment product. Together, these tools help Rogers' group monitor network traffic to scan for virus activity and remove devices from the network when necessary.

The university also uses Cisco's NAC Appliance to monitor devices on the wired network of the residence hall on its St. Petersburg campus. With more devices using the network every semester, Rogers knows the university will need better tools for identifying traffic and unusual patterns.

"We are doing well, but we can do better," he says. "It's more of a budget and time constraint issue than anything else."

## The Fine Print

Organizations that grant employees the privilege of bringing their own mobile devices into the workplace must create policies that govern which devices are acceptable, how they can be used and what applications they can access, says Cesare Garlati, vice president of mobile security at Trend Micro. Garlati suggests other important elements of a BYOD policy:

- Users must agree to install whatever security, monitoring or tracking software the organization requires.
- All devices connecting to the network must be registered with the IT department.
- Users must agree to password-protect the device.

- Use of the mobile device must impose no tangible cost to the organization.
- Use of the mobile device must not have an adverse impact on the user's performance.
- All devices must support IEEE 802.1X authentication.
- Only approved apps may reside on the device. Blacklisted apps are generally considered security or productivity risks.
- All devices must meet minimum specifications for hardware, operating systems and device management agents.

Higher Ed Scope
For more stories on colleges in Florida | Pennsylvania

About the Author
Karen D. Schwartz
Karen D. Schwartz is a freelance technology writer based in the Washington, D.C., area.

## 0 comments

0 Stars

Leave a message...

Discussion Community

No one has commented yet.

**Classroom**

Does Distance Learning Encourage Cheating? [Infographic]

Affordable access to online learning creates new opportunities for cheating.

Will Technology Push Colleges Away From the Traditional Lecture Model?

A new survey by CDW•G finds that students learn best when professors use a mix of…

…more

**Infrastructure Optimization**

Client Virtualization Saves Money and Improves Performance

Universities cut costs and run desktops more efficiently with client virtualization.

Trend Micro Deep Security 8.0

New software lets IT shops manage security with ease in virtual environments.

…more

**Security**

What Colleges Can Learn from Mat Honan’s “Epic Hacking”

Simple security measures can prevent digital catastrophes.

Review: Symantec Endpoint Encryption Device Control, Full Disk Edition and Removable Storage Edition 8.2.2

Get control of your organization’s data security policies.

…more

**Storage**

Colleges Use Storage Virtualization to Support Distance Learning

As colleges expand online learning, storage takes center stage — and virtualization makes…

5 Strategies for Deploying Deduplication Effectively

Deduplication can save space, time and money, but it must be done correctly.

…more

**Networking**

Increase in Devices Causing Bandwidth Trouble on Campus [Infographic]

How can IT departments keep up?

Dark Fiber Delivers for Columbia College Chicago

An upgraded network at the noted arts and film college gives students and faculty the…

…more

**Mobile**

Call Me, Maybe? The College Student’s Affair with Smartphones [Infographic]

How are students using their high-tech smartphones?

3 Ideas to Make the Most of Mobile Apps on Campus

Students already have the devices, so how can schools embrace the trend?

…more

Classroom

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management