The Impact of BYOD in Education

BRADFORD NETWORKS

Contents

Introduction 1

Survey Methodology 1

Key Findings 2

BYOD in Education Today 3

BYOD Adoption Across Education 3

Types of Devices Allowed 4

How Personal Devices Are Being Used 5

Network Access Control for Users and Devices 6

How Personal Devices Connect to the Network 6

The Role of NAC in BYOD 6

Provisioning Network Access Based on User Role and Device Type Policies 7

Updating the BYOD Policy 8

Mobile Device Security 9

Security Concerns about Specific Devices 9

Requirements for Anti-virus Software 9

To BYOD or Not to BYOD 10

The Demand for BYOD 10

Future Plans to Allow Personal Devices on the Network 10

Why Personal Devices Are Being Denied Access 11

The Future of BYOD in Education 12

Best Practices for BYOD in Education 13

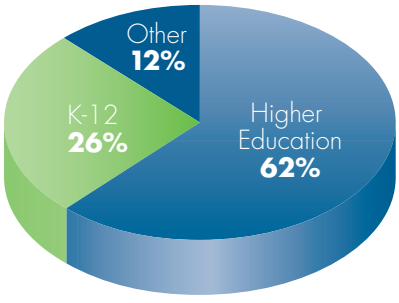
Introduction

The Bring Your Own Device (BYOD) movement has received a lot of attention in recent years. People depend on their personal devices, and they want to be able to use them everywhere to make their lives easier and more productive.

One of the biggest markets driving the adoption of BYOD is education. The BYOD model got its start in colleges and universities, spurred by technology-savvy students who demanded it and by school administrators who recognized that allowing network access using personal devices was a competitive advantage. In higher education, BYOD has become part of the fabric of student life, used everywhere from dormitories to classrooms, labs and recently in new innovative spaces designed specifically for online learning and collaboration. For their part, K-12 schools are in a transition, shifting from initially prohibiting mobile devices to increasingly embracing the BYOD concept.

As BYOD adoption increases, educators at all levels are finding new ways to integrate mobile devices into the educational experience. In both higher education and K-12, the ability to put information technology in students' hands is revolutionizing the way they learn. It is also enabling more innovative use of technology in the classroom by displacing traditional lectures, textbooks and even testing with new, interactive models. BYOD, while making this transformation possible, is also creating new challenges and questions for IT departments that are now required to enable and support the movement.

Where does the BYOD movement stand now? Bradford Networks decided to find out by commissioning a survey to better understand the current state of BYOD in education. The survey examines how BYOD is being used, challenges and concerns that are impacting wider adoption, and the potential going forward.



Survey Methodology

The survey questioned IT and networking professionals representing colleges/universities and K-12 school districts in the US and UK. The survey received responses from over 500 institutions, of which 62 percent were from higher education, 26 percent were from K-12 school districts and 12 percent were classified as "Other." The results reveal some intriguing data points about how BYOD is being used as well as future trends and opportunities.

Key Findings

- There is wide acceptance for at least some level of BYOD across all educational institutions. More than 85 percent of institutions surveyed allow some form of BYOD, and only 6 percent report no plans to implement it in the future.
- The technologies that students are bringing to school are extremely diverse—from traditional laptops to various flavors of smart phones and tablets, and recreational devices like gaming consoles and internet TVs.
- Devices aren't just for personal use; they're increasingly being integrated into the classroom and learning experience. This trend will see a lot of attention in coming years as educators take advantage of personal mobile devices as part of the 21st Century Classroom and other teaching initiatives.
- Security continues to be a top concern for many organizations. The survey also found evidence of questionable security practices that have been implemented, creating network vulnerabilities for many respondents.
- Uncertainty about how to manage network visibility and control is preventing some institutions from utilizing BYOD at its full potential.

BYOD in Education Today

85% *of educational institutions currently allow students, faculty or staff to use personal devices on their network.*

BYOD Adoption Across Education

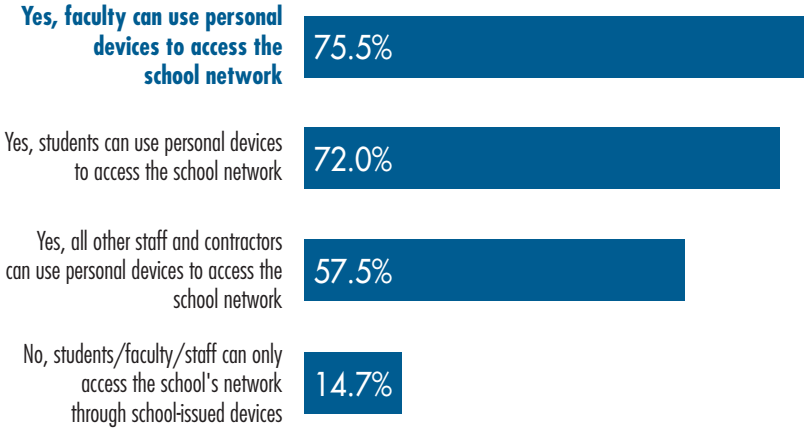
The survey reveals wide acceptance for at least some level of BYOD across all educational institutions. Less than 15 percent block BYOD completely, requiring students, faculty and staff to access the school's network through school-issued devices.

72 percent of respondents said that students can use personal devices on the school network. Adoption is most widespread in colleges and universities, where the BYOD movement first took off, with 89 percent allowing students to bring their own devices on campus. Figures are lower for K-12 districts, with 44 percent allowing students to bring their own devices. This is still a sizeable number, and reflects a changing mindset for many K-12 schools that have long been wary about allowing personal devices on their network.

» In the past, if a student pulled out a smart phone, the teacher took it away and gave it back a week later. We've gone beyond those days. We want our students to be able to connect, not only at home when doing homework but during the school day, during lessons. «

— *Phil Scrivano, Chief Technology Officer, Las Virgenes Unified School District*

Do you currently allow students/faculty/staff to use their own devices on your network?



Types of Devices Allowed

For institutions where BYOD is allowed, laptop PCs and leading mobile phone and tablet brands are supported on the network at a very high level. Since laptops and tablets are already extremely popular as learning tools, the case for BYOD for these devices is easiest to make. For example, 96 percent of schools allow personal Apple iPads and almost 95 percent allow laptops. Approval drops off sharply for devices that are primarily recreational such as gaming consoles (33 percent) and Internet-based Smart TVs (21 percent).

»The learning environment is evolving with the rapid adoption of technology. To allow for this evolution, we needed to provide our students and faculty with a secure way to access the network using personal devices, whether it's a laptop, iPad or smartphone. Immediately after deploying NAC, we were shocked to see the sheer number of rogue devices on our network. NAC has allowed us to identify these endpoints, detect security threats and manage network access.«

— *Frank Fletcher, Associate Superintendent of Support Services, Chandler Unified School District*

Devices Allowed on the Network

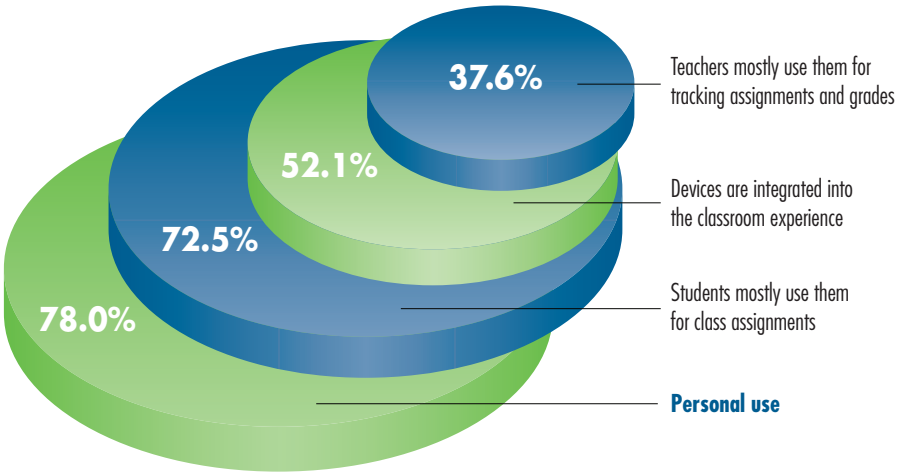
Apple iPad	**96.1%**
Personal laptop/desktop	94.6%
Apple iPhone	92.8%
Android phone	89.9%
Other tablet devices	86.3%
Blackberry phone	82.4%
Gaming consoles	33.3%
IPTV	20.7%
Other	3.6%

How Personal Devices Are Being Used

When asked how personal devices are being used in their school system, the most common response was "for personal use by teachers and students" (78 percent) followed closely by "students using their devices for class assignments" (72 percent). These results came as no surprise since personal devices have always been used for these activities.

However, one of the most exciting findings in this survey is that more than half (52 percent) of respondents reported that personal devices are integrated into the classroom experience. This suggests that BYOD is helping to enable the 21st Century Classroom, a new era in education where participants use their personal mobile devices to enable new ways of learning, teaching and collaborating. In the next few years, this is where very exciting developments will take place as educators adopt new ways to engage students and transform the classroom experience. We will also likely see new building designs where traditional classrooms and lecture halls are replaced with interactive teaching spaces that allow students and teachers to better engage with each other and collaborate in innovative ways.

How are personal devices used in your school system?



Network Access Control for Users and Devices

56% *of institutions surveyed are using a Network Access Control (NAC) solution for self-registration and to automate BYOD.*

How Personal Devices Connect to the Network

When hundreds or thousands of students converge on a school or campus, often with multiple personal devices, it creates new challenges for IT departments responsible for safely allowing users and devices onto the network.

More than half (56 percent) of respondents said that their institutions are using a NAC solution to automate the device on-boarding process and automate network access according to pre-defined policies. This indicates broad recognition that NAC software can provide secure access control for large numbers of diverse users and devices while making life easier for IT staff.

> »Over the past 12–18 months, the technology has become indispensable. Five years ago it would have been difficult to imagine us dealing with the current BYOD trend in the way we now are. Without a flexible and scalable NAC solution in place, it would have been unachievable.«
>
> *— John Cannon, Network Manager, Liverpool John Moores University*

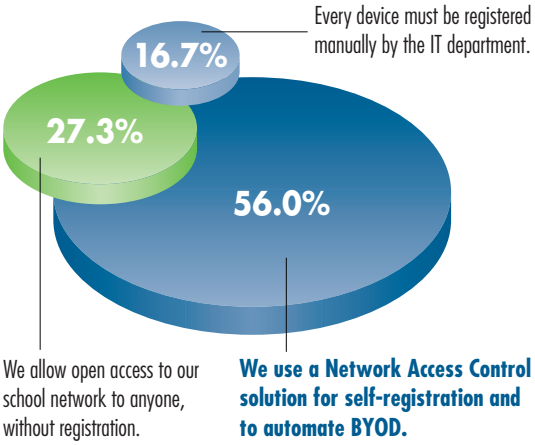
Only 16.7 percent of respondents report that user devices are registered and onboarded manually, indicating that the vast majority of educational institutions (and their IT staff) have determined this approach is inefficient. However, more than a quarter (27 percent) of respondents report that they allow open access to anyone. This suggests that they are only using BYOD for internet access, or they're throwing caution to the winds by allowing unknown devices and users into the internal network.

The Role of NAC in BYOD

Network Access Control (NAC) software plays a pivotal role in BYOD by providing automated network visibility and policy-based access control that would be very difficult or impossible for IT departments to handle manually. The result is the ability to securely on-board and manage personal devices on a massive scale, with minimal burden on IT staff.

NAC technology can identify every device and user accessing the network to make sure that only authorized users and approved devices can connect, and go only where they belong. Access can be defined by user role (student, teacher, guest, etc.), device type, location, time of day and combinations of these criteria.

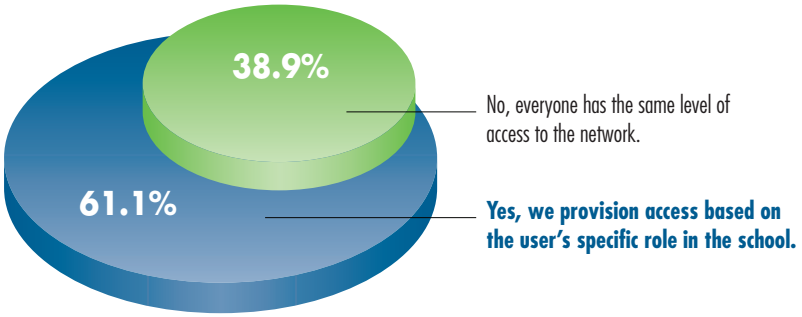
How do you currently enable personal devices to connect to the network?



Provisioning Network Access Based on User Role and Device Type Policies

More than 60 percent of respondents said their school provisions access based on user role (usually by student or faculty). However, when asked if network access is provisioned based on a user's device type, the response is overwhelmingly NO (more than 80 percent).

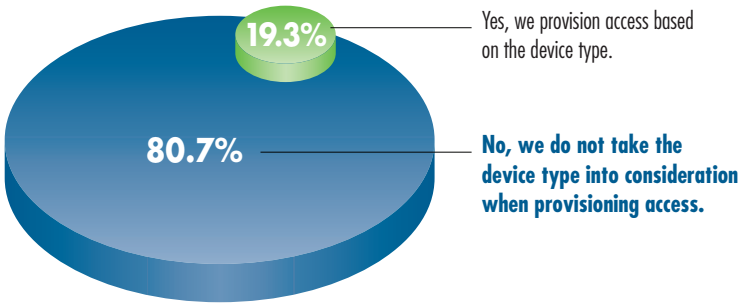
Is network access provisioned based on the user's role?



What accounts for such a disparity between the two types of access policies? A likely explanation is that the school's current wireless network management system only allows provisioning by user role, not because they don't want to provision by device type. However, without access control by user role AND by device, the picture isn't complete. When only role-based access is available, a user could access the same network resources with any device even if it does not comply with security policies or is simply not wanted on the network. For example, you probably don't want to allow a gaming console in a classroom, even if the log-in credentials of the student who owns it are valid.

Role-based and device-based provisioning work together to ensure that only authorized users with approved devices get access to specific network resources. Depending on security policies, users could also get one level of access with a school-owned device and another using a personal device. A modern NAC system can provide these capabilities.

Is network access provisioned based on the users' device type?



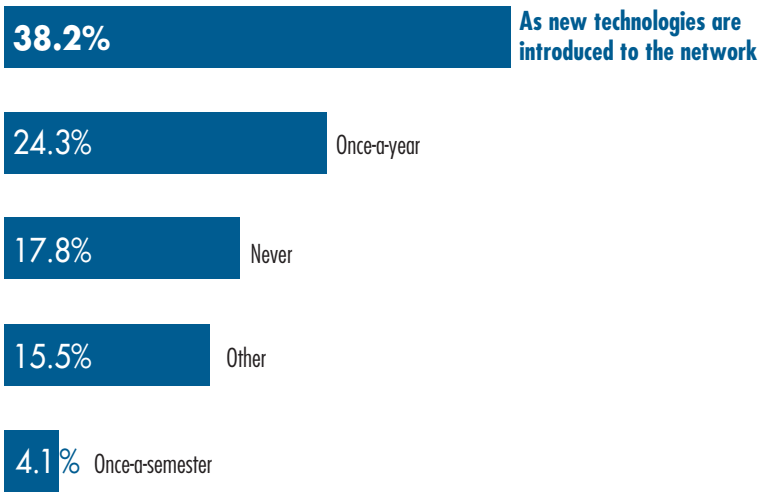
Updating the BYOD Policy

Fortunately, only a few respondents (18 percent) said that their institution *never* updates its BYOD policy. However, the other figures are also problematic.

The largest number (38 percent) said that they update their policy as new types of technologies are introduced across the school. This may seem like a sensible approach, but these aren't the only changes that can impact network performance in a BYOD setting.

Most networks undergo a steady stream of changes including: proxy changes, configuration changes and technology changes. In this dynamic environment, a BYOD policy can quickly become out-of-date. Access will then become either too restrictive (users won't be able to get the resources they're entitled to) or too open and unsecure (allowing users and devices to go where they don't belong). For all these reasons, BYOD best practices dictate that educational institutions should review their BYOD policy at least twice a year and update it when necessary.

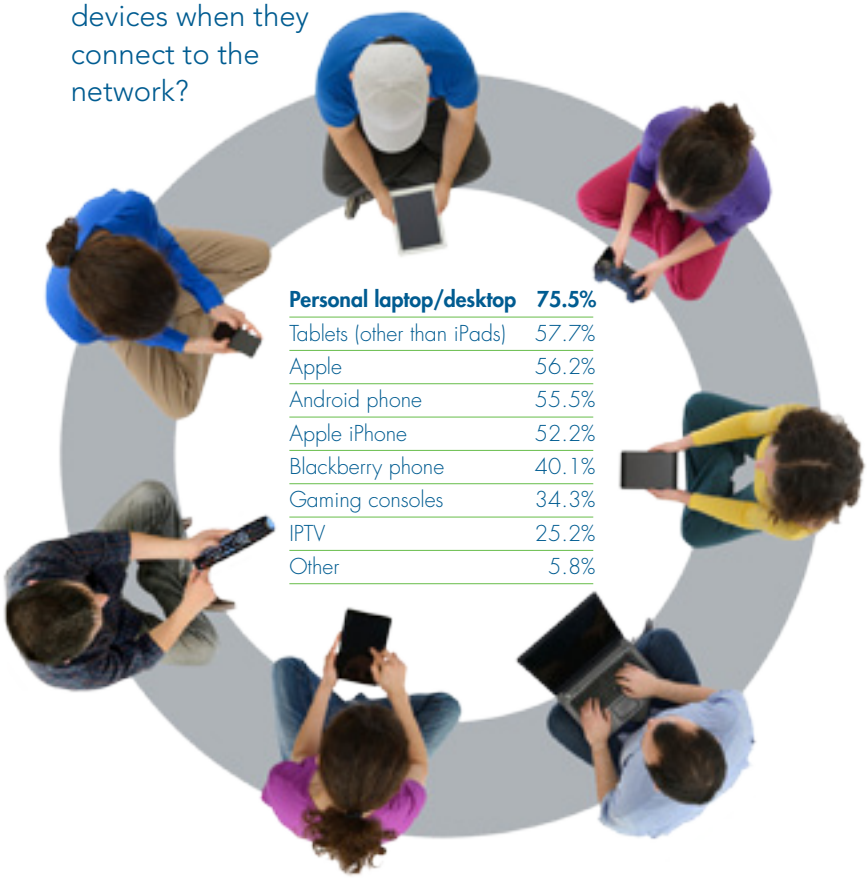
How often do you update your BYOD Policy?



Mobile Device Security

46% *require an anti-virus product be installed on a personal device before allowing it to connect to the school or campus network.*

Are you concerned about any of these specific devices when they connect to the network?



Personal laptop/desktop	**75.5%**
Tablets (other than iPads)	57.7%
Apple	56.2%
Android phone	55.5%
Apple iPhone	52.2%
Blackberry phone	40.1%
Gaming consoles	34.3%
IPTV	25.2%
Other	5.8%

Security Concerns about Specific Devices

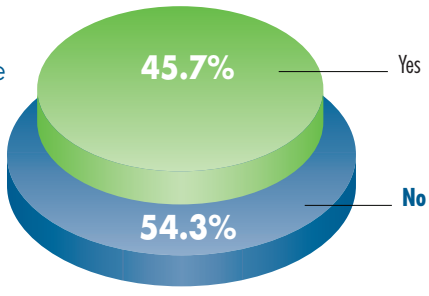
While the survey determined that many different device types are allowed network access, there are significant reservations about security. Laptops and desktops are the biggest concern (more than 75 percent), perhaps due to a perception that they're more susceptible to viruses. There are also major security concerns regarding tablets (57 percent) and Apple iPads (56 percent).

Requirements for Anti-virus Software

Less than half of respondents (46 percent) require anti-virus software to be installed on a personal device before allowing it on the network. We can only assume that these institutions are only allowing internet access from user devices, and keeping the internal network off limits.

We may also surmise that IT personnel have no easy way to check each device to see if anti-virus software is installed or up to date. While they may recommend anti-virus software for personal devices, they can't enforce it. To enable safe access into the network, they need the ability to detect if a device has the right anti-virus software and meets other configuration requirements, restrict access if it doesn't, and provide easy remediation that users can do themselves with a few taps or clicks.

Do you require an AntiVirus product to be installed on the device prior to allowing it to connect to your network?



To BYOD or Not to BYOD

84% *of those institutions that currently don't allow BYOD receive requests to use their personal devices on the network.*

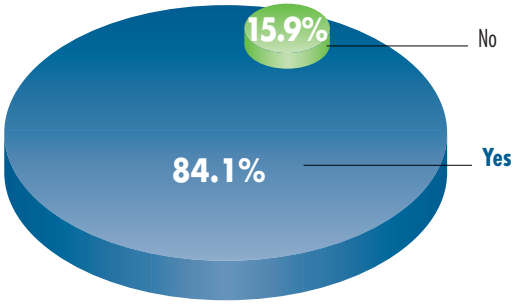
» During the next five years, BYOD is on its way to becoming the prevalent practice in educational settings at all levels—in K-12 and higher education venues alike. Whether it acts as a disruptive trend or constructive strategy will depend heavily on if and how CIOs and system administrators plan for it. «

— Bill Rust, research director, Gartner, Inc., BYOD in Education by Design, Not Default, May 2012

The Demand for BYOD

Survey results show that students and staff are clamoring for BYOD. For institutions that don't currently support BYOD, 84 percent report that students, faculty and staff are demanding to use their personal devices on the school network. The vast majority of these institutions are K-12 schools, suggesting that the adoption of BYOD in this segment is likely to grow.

Do you receive requests from students/faculty/staff to use their personal devices on the school network?



Future Plans to Allow Personal Devices on the Network

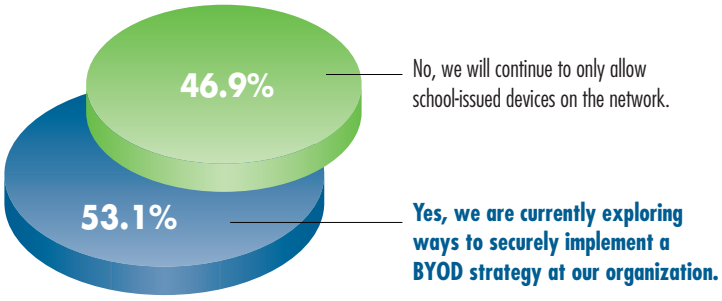
This question, like the previous one, was aimed at that 14 percent of institutions that don't currently offer BYOD. Of those, less than half (and less than 6 percent of the total overall) have no plans to allow personal devices on the school network.

Schools need to recognize that BYOD is happening whether they like it or not. Even if they refuse to allow it, technology-savvy students (and sometimes teachers and even staff) are probably doing it anyway, under the radar. Besides, banning personal mobile devices can hinder education and effect recruitment.

Rather than resisting BYOD, a better approach is to manage it and take advantage of it while ensuring the safest possible school environment. Allowing students to bring their personal devices is also the key to new approaches like flipped classrooms, blended learning and the

21st Century Classroom mentioned earlier. Another idea gaining traction is a move to digital textbooks that engage students with rich online learning experiences in ways traditional textbooks never could. Online textbooks have already taken hold in South Korea and other countries, and the U.S. Education Secretary has urged educators to make the transition as quickly as possible.

Do you have any plans to allow students/faculty/staff to use personal devices on the school network in the future?



» Over the next few years, textbooks should be obsolete. The world is changing. This has to be where we go as a country. «

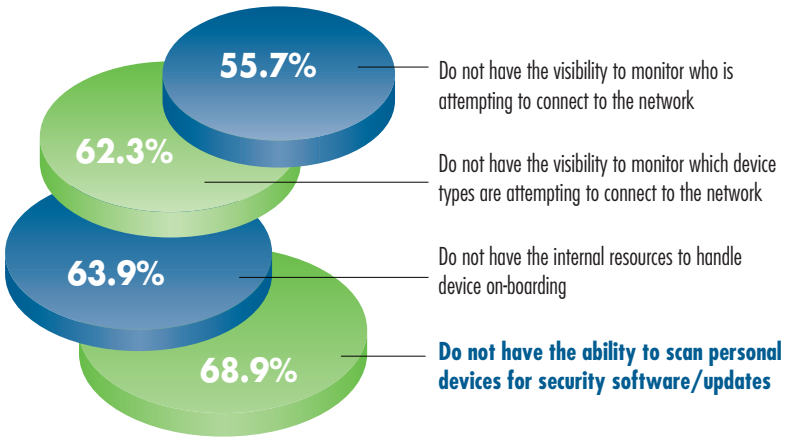
— *Arne Duncan, U.S. Education Secretary, October 2, 2012, remarks made at the National Press Club*

Why Personal Devices Are Being Denied Access

The survey also examines the main reasons why some educational institutions block personal devices from accessing the campus network. As the chart reveals, there are significant concerns about the ability to manage large numbers of users and devices trying to access the network. 69 percent of respondents say they are unable to scan personal devices for security software/updates, while 62 percent do not have the visibility to monitor which device types are attempting to connect to the network. In addition, 56 percent do not have the visibility to monitor who is attempting to connect, and more than 60 percent say they lack the resources to handle on-boarding even if the institution is willing to allow it.

Technology is available that addresses each of these concerns and makes secure, highly automated BYOD a practical reality. With automated visibility and control, IT departments can offer the benefits of BYOD on a school or campus network, without the risks that have held them back until now.

What are your reasons for blocking personal devices from accessing the network?



The Future of BYOD in Education

The survey results ultimately reveal two key findings about the state of BYOD in education:

1. There is strong evidence that BYOD is a dominant model in educational settings at all levels. Putting technology in students' hands is transforming the educational experience, not only in colleges and universities, but in K-12 schools as well. BYOD is fueling the transition as educators move from traditional lecture-based instruction to new models of learning, teaching and collaboration. Rather than resist this revolution in education, results suggest that more and more institutions are embracing it.

2. There is considerable uncertainty about how to make BYOD work. The survey revealed some questionable security practices as well as possible misconceptions about the right way to handle security when students are bringing their personal devices to school. Not all institutions were aware of the importance of visibility into both users and devices accessing the network, or the access control measures needed when thousands of varied users and devices are trying to get on the network. These are areas that schools and universities will have to address if their BYOD initiative is be a success.

Whether the setting is an elementary school classroom or a college dormitory, the BYOD process needs to be seamless and automatic, and able to provide visibility and access control on any scale. For students, teachers and other users, this means simple on-boarding so they don't need to worry about how to get on the network. For IT staff, it means the ability to identify every user and device trying to access the network, with granular access control to make sure that users are getting the specific resources they need, when and where they need them, yet prevent them from accessing resources for which they do not have permission. Technology is now available that can address these challenges and bring the benefits of secure BYOD within reach so schools can participate in the dramatic changes sweeping education.

» Until recently, many educational institutions have treated BYOD as a trend, taking a laissez-faire approach. In the future, they must shape BYOD into a thoroughly thought-out and defined strategy — a strategy that addresses the challenges and leverages the multiple benefits that BYOD can provide. «

— Bill Rust, research director, Gartner, Inc., BYOD in Education by Design, Not Default, May 2012

Best Practices for BYOD in Education

Based on extensive experience developed from helping over 600 educational institutions, Bradford Networks recommends the following best practices when developing a BYOD solution:

1. **Conduct an in-depth analysis of your network visibility and security**
   - How much visibility do you currently have into who and what is connecting to the network?
   - Can you identify the types of endpoint devices that are connecting, as well as who is using those devices to connect to the network?
2. **Create or update your BYOD policy**
   - Decide which devices you will support (iPads, smartphones, PlayStations, Xbox, IPTV, etc.)
   - Determine which operating systems you will support, and which AV software you will require (and their versions). Allow at least one "free" antivirus option whenever possible.
   - Decide whether you will prohibit or restrict any specific applications (such as Peer-2-Peer music sharing)
   - Determine the different role-based access policies needed for faculty, staff and students
   - Determine remediation policies — such as isolation or limited access
   - Set up remote registration so that students can pre-register their devices before they leave home.
   - Keep the process simple — remember that students get frustrated easily
3. **Implement in phases**
   - Start with problem areas that are high risk
   - Expand into other areas
4. **Provide a solution for guests**
   - Make guest access easy to find and connect
   - Limit guest access (network and bandwidth), or guest networks may become overused and overloaded
5. **Communicate the policy**
   - Keep it simple: the fewer words the better
   - Make sure all stakeholders know the policy requirements
   - Offer assistance (give them a supervised place to go when they get frustrated)
   - Let them know you are just ensuring compliance

One of the most important things to remember is that you can't just set up your policy based on a snapshot of security risks and student/faculty needs at a single point in time. BYOD is an ongoing process: You must continuously check for the changing needs of users, and modify your policy accordingly. Using the right technology solution is a key factor in ensuring your policy is up-to-date and network access is automatically managed. Network access control gives your IT department the ability to manage and secure the BYOD tsunami, while enabling students and faculty to take education beyond the classroom walls.

BRADFORD NETWORKS

Bradford Networks is recognized as the vendor of choice for educational institutions that are proactively addressing the security and management challenges of BYOD. The company's Network Sentry solution is the first network security offering that automatically identifies and profiles all devices and all users on a network, providing complete visibility and enabling total network access control. Today, millions of students around the globe are using Network Sentry to gain access to school and campus networks, safely and automatically.

For more information, please visit **www.bradfordnetworks.com**.

One Broadway, 4th Floor, Cambridge, MA 02142, USA

Toll Free +1 866.990.3799 | Phone +1 617.401.2515

Email info@bradfordnetworks.com

Web www.bradfordnetworks.com