

The BYOD Revolution:

Key to Improved Employee Learning, Engagement and Collaboration

Want more productivity from your knowledge workers? Join the BYOD (Bring Your Own Device) revolution, AKA “the consumerization of IT.”

- **Do** let employees access the company’s resources through their personal devices rather than via company-issued products while at work.
- **Do** let them be productive at home or on the road by using their devices to connect with the company’s systems.
- **Don’t** let the fear of cyberattacks or of compromised security deter you because these problems can be controlled.

BYOD: Employees Loving It

Many learning leaders don’t fully appreciate the emotional connection employees today have with their personal devices. They’re joined at the hip with them, both literally and figuratively, and they put enormous value on the availability of 24/7 connectivity.

Many learning leaders also aren’t aware of how much time employees spend working after hours – work that can be made much more productive with improved connectivity.

The research results are startling: The average employee puts in more than a month and a half of overtime each year, or seven extra hours each week. Half of Americans can’t even put their phones down while in bed. (This has become so commonplace that only a quarter of those polled said it caused an “occasional disagreement” with their partner.) Some two thirds of people check their work emails before 8 AM, two fifths still work after 10 PM, 38 percent check email while at the dinner table and seven in ten won’t go to sleep without checking. Anti-BYOD policies are blocking these employees from giving their full effort to the business.

Millennials are particularly wedded to their devices, as they are to all the new communications technologies. Research shows that one in three millennials values social media freedom, device flexibility and work mobility more than they do salary when accepting a job offer. They switch their attention between media platforms like

smartphones, laptops, tablets and television an average of 27 times per hour. Some 47 percent can't go a day without SMS and one third can't last the day without social networking. Some 58% worldwide believe BYOD is a right, not a privilege. A report last year concluded that one in three college students and young professionals considers the Internet as important as air, water, food and shelter. Remarkable!

This is the age of hyper-connectivity: the average knowledge worker uses 2.8 devices and by 2014 the average will be 3.3.

Don't cut the employees' connectivity with the company by prohibiting them from using their devices for work.

The Many Uses of BYOD

Businesses are making impressive productivity gains by letting employees use personal devices to access company documents, attend meetings, deliver multimedia assignments, collaborate with co-workers, share information, store contacts and manage their calendars. Employees greatly prefer the personal devices they've selected not only because they're their own but also because, in the vast majority of cases, they're superior to the company-issued product.

Employees upgrade to the newest improvements much more quickly than the tortoise-paced upgrade rate used by most businesses. Why a company would want employees to work at less than peak productivity is one of the great mysteries of business today.

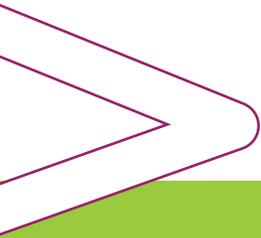
BYOD for Learning

Businesses are making particularly impressive gains in the effectiveness of their learning programs by incorporating BYOD capabilities in employee training. Irrespective of their location, facilitators are able to launch presentations that tap into a wide range of company resources as well as web-based applications. Logical Operations' LogicalCHOICE training system provides facilitators with multi-platform

instructions and recommendations for each lesson in their facilitator guides – content that they can access anywhere, anytime with their devices.

Training centers no longer have to provide computers preloaded with software for the student. Students can download the needed hardware right onto their device, virtually. This reduces hardware costs and IT resources significantly.

Using their devices, students are able to learn the way they prefer to learn. They can access many external materials, including supplemental study guides, workbooks and textbooks. Post-training, they can continue to dialogue with the facilitator and classmates. In this way, BYOD increases retention of the skills taught, accelerates the movement of skills learned in the classroom into the workplace and fosters the kind of collaboration that creates innovations. Altogether, BYOD provides faster adoption of newer and better ways to work and forever changes the culture.



BYOD Policies Needed

A new study reveals that three quarters of surveyed organizations around the globe now allow employees to use their own devices for business.

But BYOD isn't an unalloyed blessing. Some IT directors say BYOD stands for Bring Your Own Disaster. The potential for serious damage certainly exists.

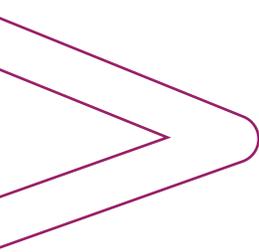
For example, employees who use a smartphone to access the company's network and then lose the phone can cause confidential data stored on the phone to fall into the wrong hands. This data might include product development plans, customer lists and revenue projections. BYOD also can increase vulnerability to cyberattacks.

Clearly, the BYOD-friendly business needs policies to protect itself. Make sure your BYOD policy establishes:

- Whether there should be a separate network designed solely for mobile devices.
- What devices and apps are acceptable, which of them can be used for the enterprise network and what kind of registration process is needed.

- Whether or not social media posts can be made during business hours.
- What happens with e-mail passwords and access tokens when an employee leaves the company.
- What happens when an employee loses a device. How soon must the company be notified when this happens. Company data must be wiped out but how should the “force wipe” be conducted so personal content, like family photos, is preserved?
- How to prevent unauthorized access to employees’ personal information.
- How to prevent access to the enterprise network by an unauthorized user of an authorized device.
- How to prevent malware from infecting the mobile device and subsequently the enterprise network.
- What’s the best way to protect against the bypassing of passwords or the use of too-easy passwords.
- How much should bandwidth be increased.
- How best can the company track mobile device uses.
- How should the company comply with regulations that may require written notification to users that their online activities are being monitored.

Some companies have created the position of chief mobility officer to create and monitor BYOD policies. Using the genius bar in Apple’s retail stores as a template, they are creating mobile shops that help employees connect their devices to corporate resources.



Who Should Own the Devices?

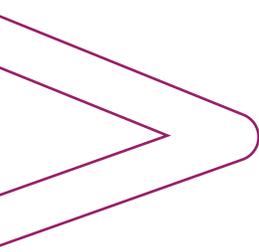
At most companies the employees do. This helps get the company out of the business of buying hardware and supporting it. At some companies employees can

apply for an interest-free loan to buy their devices. Other businesses pay the monthly service fees for the products; the employees agree to let the company install security software that removes data if the equipment is lost or stolen.

Some companies have purchased the devices for a low fee to give them legal control of it. Some give employees responsibility for security protections such as keeping antivirus software current, with IT typically responsible only for troubleshooting problems associated with corporate software, not the operating system.

Making employees responsible for the security of their devices helps guard against sensitive information getting to an employee-owned product.

In some businesses HR staff members can no longer copy a file with sensitive employee information to a laptop that goes home.

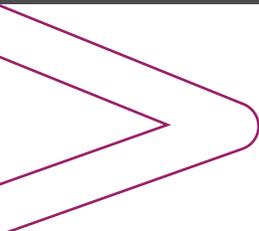


BYOD Will Drive More Change

As more employees use mobile devices rather than desktop PCs, it's likely that there will be more remote workers. This will reduce costs for office space, equipment and power usage. The more-distributed workforce will provide access to a broader talent pool.

It's clear that the increasing use of mobile devices will drive more wireless network traffic. This means businesses will have to increase their mobile and wireless capacity. They may have to invest in wireless printers. They may need to put more effort to combating repetitive stress injuries from personal devices rather than desktops.

We haven't begun to see the extent of the changes the BYOD revolution will bring.



Reference Sources

“The Case for BYOD in the Classroom,” **Logical Operations, Inc., 2012**

“How to Bridge the Gap from Traditional Training Delivery to the Virtual Classroom,” **Logical Operations, Inc., 2012**

“Let’s Encourage BYOD in Training,” **Training Magazine, August 30 2012**

“Good Technology Survey Reveals Americans Are Working More But on Their Own Schedule,” **Good Technology Press Release, July 2 2012**

“BYOD: If You Think You’re Saving Money, Think. Again,” **CIO Magazine, April 4 2012**

“BYOD Myths: Cost Savings, Productivity Gains, Less Headaches,” **CIO Magazine, April 11 2012**

“Cisco helps users welcome BYOD,” **Network World, March 30, 2012**

“Security Challenges of BYOD and Gen Y,” **Baseline, June 26 2012**

“Mobile & Wireless Slideshow: BYOD Finds Fans in IT,” **CIO Insight, June 5 2012**

“Bring Your Own Device: More Employers Are Allowing Employees to Use Their Own Technology in the Workplace,” **Social HR Home, March 15 2012**

“California’s budget crisis sparks controversial ‘BYOD’ plan to save money,” **Network World, June 8 2012**