

Blog for TTI

<http://www.ttihouston.com/blog/bid/397724/Joining-The-BYOD-Party-Know-The-Details-First>

Joining The "BYOD" Party? Know The Details First

Posted October 7, 2014

Remember the day when the last desktop computer vanished from your office? Of course they were originally replaced by company-issued laptops, which made portability between cubicles, conference rooms, and offsite tasks much easier. But as the functions of portable computing evolved — and spread into modern smartphones — many employees have become frustrated with the "Model T" approach of many IT departments: "any device you want, as long as it's whatever we give you."



This led to one of the most rapidly-growing trends in business IT today: Bring Your Own Device, or BYOD. In BYOD systems, every eligible employee receives a company subsidy to purchase their own mobile device for work, whether that's the latest-and-greatest notebook/smartphone or another cost effective option. Often called the "consumerization" of IT, BYOD enables the end user to custom-tailor their personal work tools.

Reasons to Switch

More and more companies of all sizes are transitioning to a BYOD policy for their workforce, for several key reasons:

- Savings from not purchasing whole batches of new devices.
- [Choosing a device](#) — for onsite use or work-from-home telecommuting — tends to help an employee feel more "in control" of his or her career, ultimately boosting overall productivity.

- Managers avoid the (often awkward) process of retrieving "company property" from a departing employee.
- Unused surplus equipment won't sit gathering dust in a back storeroom as it sinks into obsolescence.

While a BYOD environment has plenty of benefits, it also comes with a few serious legal and technological considerations. Before cutting stipend checks and sending employees to their favorite electronics retailer, a company must lay crucial groundwork:

Update Acceptable Use Policies

Legal agreements which governed traditional "fixed" hardware need to be updated and expanded to define acceptable use for [BYOD devices](#), which will likely be used for employees' personal needs beyond work. Avoid cookie-cutter legal templates and consult stakeholders — top management, legal, and IT — to craft a document which safeguards company data while firmly defining business and personal uses.

Future-Proof Your Network

As your business grows, so will the demand from employees and BYOD policies. The ever-evolving spectrum of devices will continue to demand greater amounts of network traffic to deliver crystal-clear VoIP, high-def images, video, and other bandwidth-hogging applications we likely haven't even imagined yet. Strengthen your LAN infrastructure to handle tomorrow's mobile computing.

Self-Service Onboarding

Activation and customization of a new mobile device should be as user-friendly as possible, with minimal IT assistance. Online start pages and help files should span a "common denominator" of operating systems, from Apple OS and Android to those final die-hards of Blackberry. Be prepared for those frequent system updates which may cause glitches with older apps.

Your Own Company "App Store?"

Whether it's a new hire or a long-time employee customizing their new device, there will be plenty of downloading new software, from IM and video/audio conferencing platforms

to file-sharing and collaboration tools. Employees often rely on piecemeal links emailed from co-workers or take chances on unknown third-party apps, which may harbor intrusive malware or viruses. By creating a specific mobile company homepage or similar online hub or portal, those employees can easily find download links to "tried-and-true" applications vetted and officially approved by IT.

Enable The "Kill Switch"

If a device is lost or stolen, IT should have the ability to employ remote wipe technology to instantly render all encrypted data unreadable. Similarly, while a terminated employee may keep their personal hardware, any sensitive company data on the device will be rendered unreadable. A company should only use this feature when clearly within its purview and the condition should be included in the new Acceptable Use Policy.

So as we've seen, Bring Your Own Device adds another dimension to today's enterprise mobility. Remembering to iron out all the details in advance will help to eliminate complications after allowing employees bring their devices. BYOD policies should cover much more than business phone systems and your VoIP system, expand your reach to cell phones, laptops, and third party apps for optimal security.