A Smarter Approach to Mobile Device Management

INFINITY

A Smarter Approach to Mobile Device Management

How Can You Protect Your Data When It's Being Accessed and Shared in so many Different Ways

With Great Mobility Comes Great Responsibility

More and more people today are using their personal mobile devices like smartphones and tablets for business purposes. Such devices, coupled with greater Wi-Fi accessibility and cloud services, have empowered us with the ability to access data and do business from practically anywhere at anytime.

Needless to say, many small-to-medium-sized business owners have embraced the BYOD (Bring-Your-Own-Device) revolution. The benefits are obvious: increased employee productivity, enhanced services to customers/clients, and better overall customer and employee satisfaction.

But what about the potential consequences associated with this mobility revolution? Are small business owners doing enough preemptive planning to address potential risks that could arise with the use of personal devices?

Mobile Device Management - Questions Every SMB Should Ask

First, it is important that small business owners honestly assess whether their systems, networks, data, and overall infrastructure are ready for the use of an array of mobile devices.

Once it is firmly established that both internal IT and components in the cloud are prepared for BYOD, solutions should be put into practice that are concurrent with terms-of-use policies or any guidelines pertaining to remote/telecommute workers or the sharing of sensitive data. The following questions should be answered to ensure the best mobile device management for your business.

14+ billion
mobile devices projected in service globally by 2020

Nearly 40%
of companies do not have a BYOD agreement or policy

Trustlook

What particular devices or applications are permissible for work use? Assuming security requirements are in place, not every device or application will meet those.

Will anyone in the company be tasked with the daily management of BYOD strategies?

What should BYOD policies cover, and what kind of management solutions will be needed?

Would a BYOD management tool that collects device information, deploys and monitors usage, and offers insight into compliance be helpful?

Smartphones increase productivity
34%

Samsung Insights

Which costs will be the responsibility of the employee? This pertains to any fees associated with usage - from network plans, to the device itself, to software, accessories, and maintenance costs.

What data will be accessible? Will data encryption be necessary for certain information traveling through the personal devices of employees? Which employees will have read, write, update/delete privileges?

What is the process when handling sensitive data stored on lost or stolen devices or on the personal devices of ex-employees? Does the company or organization have the right to wipe out the entire device or just corporate data and apps?

BYOD is here to stay as it affords smaller-sized companies the mobility of a corporate giant without a huge investment. But when it comes to ensuring that devices, applications, and networks are safe from the variety of threats linked to greater mobility, small business owners may find it necessary to enlist the help of a managed services provider to adequately take on mobile management challenges and provide ongoing consultation. Contact your local team at Infinity, Inc. to get started today.