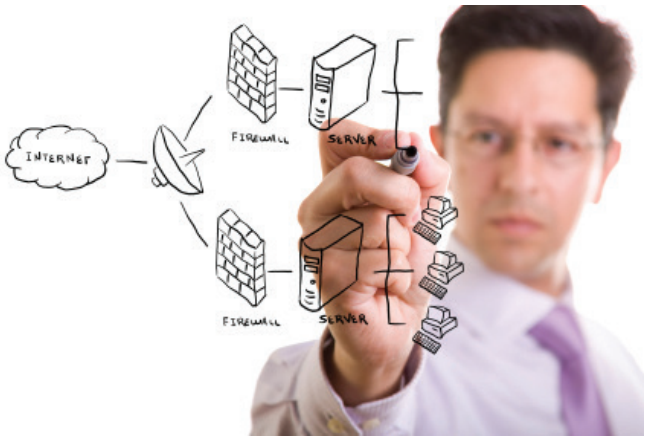
EMBRACING THE AGE OF MOBILITY

Created for Steve Van Tol

Embracing The Age Of Mobility & The BYOD Workplace



OVERVIEW

In today's always-connected world, the time-honored separation of work and personal time is quickly disappearing. Mobile devices such as laptops, netbooks, tablets, and smartphones have fundamentally changed how all of us live and work.

With work no longer confined to a physical *office space,* or limited to traditional business hours, we've created an increasingly mobile and dispersed workforce capable of working anywhere at anytime. 3 out of 5 workers today no longer believe an office presence is necessary for a productive day's work. By 2015, the IDC estimates the U.S. will have over 200 million people working remotely.

By now, it's obvious that BYOD (Bring-Your-Own-Device) isn't just another buzz-worthy acronym or a workplace trend that will eventually fade; it's part of the complete restructuring of the conventional way we've worked up to this point.

There is simply no going back to the way we were. With or without company approval, employees prefer working from devices they own and are most comfortable with, meaning it's out with yesterday's loud, clunky and slow in-office desktop PCs and in with today's feature-rich, on-the-go, employee-owned mobile devices.

Although many small-to-midsize businesses (SMBs) have fully embraced BYOD for its countless benefits, this proliferation of employee-owned devices accessing company databases, files, and email servers is unprecedented. It is also risky because it increases vulnerability to security breaches and data loss.

Which raises the question: are workplaces today responsibly ushering in BYOD with safety, security, and long-term adaptability in mind?

In this e-guide, we will examine the pros and cons of BYOD and outline five safe BYOD practices to ensure a safer and smoother transition into this age of mobility

EMBRACING THE AGE OF MOBILITY

THE MAINSTREAMING OF BYOD

It's hard to believe that just a decade ago work mobility was practically non-existent. We worked from cubicle farms with workstations and desktop PCs straight out of the movie Office Space. The office was our only access to the company network. Select employees might be provided with company-issued laptops with pre-loaded software useful for work. Perhaps they'd be trusted with FTP (File Transfer Protocol) privileges to access and transfer files to the server. Cell phones were actually just phones.

Even when BlackBerrys were introduced to the business world, allowing people to use a mobile handheld device to access their work email and manage their schedule for the very first time, the BlackBerry Enterprise Server made it easy for IT departments to configure and manage the device.

BlackBerrys eventually gave way to iPhones and Androids.

Laptops eventually gave way to iPads and tablets that combined laptop usability with smartphone portability.

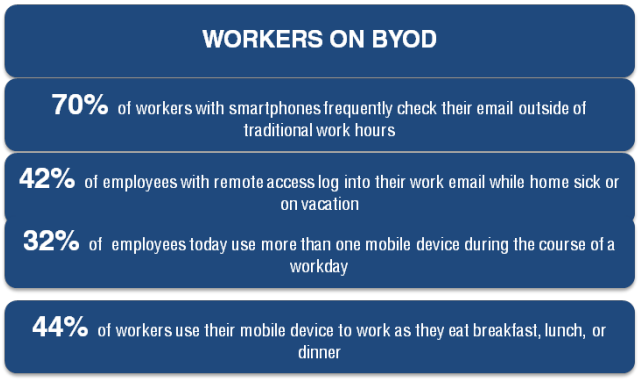
Meanwhile, the number of public Wi-Fi hotspots grew, making employees eager to access their company network and work files from just about anywhere through their mobile device.

Today, BYOD has become the "new normal". A recent poll of 1,021 small business owners in the United States found that 68% allowed employees to use personal devices for work. 79% of CIOs at businesses who aren't encouraging BYOD believe employees access their network with unauthorized personal devices every day.

Initial resistance to the BYOD movement has proven to be futile. Gartner, a technology research firm, predicts that 90% of businesses and organizations will support the use of personal devices for work purposes by the end of 2014. And it certainly seems that more business owners today are seeing the upside of BYOD, which include…

Increased Production

On average, it has been approximated that businesses gain 9 additional hours of productivity per week when employees use personal devices.



EMBRACING THE AGE OF MOBILITY

Improved Service

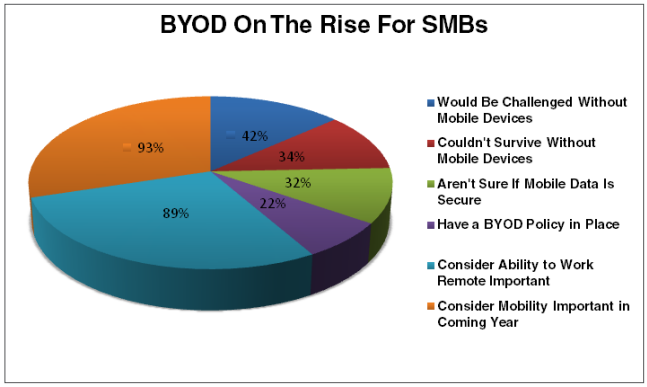
The benefits of this increased production and greater flexibility naturally extend to clients and customers since mobility allows workers to resolve escalated issues or almost instantly reply to inquiries outside of normal work hours. It is common these days to receive an email response after 5pm with a "Sent from my iPhone" tagline at the bottom.

Reduced Costs

Transferring IT hardware and equipment expenses to employees can save SMBs significant money. A study conducted by Cisco's Internet Business Solutions projected that U.S. companies utilizing BYOD can save up to $3,150 per employee each year.

Additionally, since consumers are drawn to the freshest technology, and the latest upgrade to their device of choice, businesses no longer have to budget to continually upgrade to keep up with technological advances.

In 2013, telecommunications and information technology service provider *Cbeyond, Inc.* conducted a blind survey of 711 C-level executives of firms with fewer than 250 employees. Their findings revealed that not only is BYOD more widely accepted today, but mobile devices have also become critical to day-to-day operations and essential to meeting business objectives. Many acknowledged that it would be a challenge to do business today otherwise. A fair share of executives felt their business couldn't survive without mobile device usage.



Data from Summer 2013 Cbeyond Business Leader Snapshot™ - Surveying 711 executives running businesses w/ less than 250 employees

One troubling aspect of the aforementioned report is 32% of the surveyed SMBs aren't sure if their data is adequately protected. While they acknowledge that BYOD puts their organization at risk, just 22% of SMBs currently have a comprehensive BYOD policy in place to address mobile device usage and define data privileges extended to personal devices. Here are a few reasons this sets a dangerous precedent.

- Nearly a third of employees use more than one mobile device during a typical workday. It's critical that organizations, especially small businesses, know what

devices are accessing their network and whom they belong to.

- With the existence of public Wi-Fi hotspots at coffee shops, restaurants, hotels, convention centers, trains, and airports, inadequately secured mobile devices are constantly exposed to hackers monitoring traffic on open networks. According to data compiled by the Ponemon Institute, 59% of organizations have experienced a rise in malware infections linked to insecure mobile devices.

- BYOD makes SMBs increasingly susceptible to costly data breaches with 38% of these breaches occurring as the result of lost or stolen mobile devices. Verizon Business has estimated that 174 million records have been stolen in 855 data breaches linked to smartphones and tablets.

- There are more than 500,000 apps in the Apple App Store. The Android Marketplace has over 200,000 apps. The security controls in place to evaluate the safety of these applications are suspect and some apps having phishing screens, hidden spyware, and malware. This means the apps or clients being used to access enterprise content could put your data at risk.

The adoption of BYOD can be beneficial to small businesses but it shouldn't compromise company or customer data. Developing a comprehensive BYOD policy minimizes risk while still granting full (and secure) access to the files and applications your employees need, regardless of where they are.

FIVE TIPS TO SAFE BYOD

1. Create a Mobile Device Policy and Enforce It

Don't be afraid to spell out what employees are expected to do - and not do - with their mobile devices. It's important to remember you aren't only managing devices but people as well. This is where you define acceptable and unacceptable behaviors and make it clear that there will be no exceptions.

Clearly define what types of devices are allowed. While you want to support a mix of the devices employees are most likely to carry, a line has to be drawn somewhere to prevent things from becoming unmanageable. No company, especially a small one, needs to open up things to 30 mobile devices. Minimum standards for device age and capabilities should be set. Newer technology will obviously have better security features. For instance, anything before the iPhone 3G will not permit device-level encryption.

Every policy should address acceptable personal device use when it comes to web

browsing, app downloads/usage, public Wi-Fi protocol, and data transmission/ storage guidelines.

2. Keep Devices Lock & Password Protected

Your employees are using devices they take with them everywhere. You have no idea where they are at any given moment of the day. More importantly, you can only hope that their mobile device is either with them or stored away safely. Devices that aren't password protected, which are left out in the open unattended, pose a huge risk.

Keep in mind that 46% of people who use their mobile device for work admit to letting others use it from time to time. Many devices have free built-in security controls such as locked screens, the ability to remotely wipe out the device after multiple successive failed authentication attempts, and even GPS trackability.

Passwords should be strong and frequently updated. Employees should also be advised to not keep written passwords lying around.

3. Immediately Disconnect Terminated Employees or Voluntary Leaves

Be sure to remotely wipe company data from the personal device of any employee who is terminated or voluntarily leaves the company. Ideally, this data should be retrieved. This is one reason a SMBs mobile device policy must address where employees are to edit and save files. Many SMBs these days require all files to be shared, edited, and saved on Cloud-based software like Dropbox.

4.Use Available Encryption Technologies

Business critical files, folders, and hard drives should be encrypted for reliable protection against unauthorized access. Encryption prevents sensitive data from being read by potential hackers as content is transferred to and from mobile devices.

5. Use a Mobile Device Management (MDM) Solution

MDM solutions are a cost-effective means to ensure that any mobile device accessing their network is identified, controlled, and monitored. This method of centralized management makes it easy to configure devices for enterprise access, stipulates password policy and encryption settings, locates and remotely clears and locks any lost or stolen device, automates security updates, and proactively identifies and resolves device or app issues.

EMBRACING THE AGE OF MOBILITY

CONCLUSION

Any potential return from the increased productivity and reduced operating costs associated with BYOD is nullified if sloppy management of these devices leads to expensive security breaches and data loss. While SMBs undoubtedly want to accommodate employees wishing to use their own devices, they must also guide them to acceptable and safe usage. Employees are likely to resist being told what to do with devices they own, but a secure BYOD environment is only possible if a mobile device policy is written and enforced with no exceptions whatsoever.

SMBs are encouraged to ease into BYOD a little at a time. Start with just a few employee-owned devices to test security and scalability. Always remember to keep your mobile device policy constantly updated and stay in front of emerging trends and approaching market releases.

For Additional Information Please Contact
Steve Van Tol
steve.vantol@jcmr.net
T: 704-707-3333 x3008
5950 Fairview Road Ste 140, Charlotte, NC 28210