



# Straight Talk from the Corner Office



October 2014

## BYOD 2014 - A business update -

Welcome again to *Straight Talk*, one of the ways Coranet shares perspectives on important issues and opportunities in business communications.

Our very first 'Spotlight' back in the summer of 2012 focused on the consumerization of communications technology, and discussed some of the challenges and potential benefits that have accompanied the global shift towards *Bring Your Own Device (BYOD)*. This has continued to be an area of great interest to Coranet clients. Since two years have passed, we wanted to share (in a 2-part series) some updated perspectives and lessons learned.

As a quick refresher, BYOD simply refers to the use of employee-owned devices to access company networks and information, with the main driving force being the likelihood that employees' personal devices are often more advanced and effective than company-provided technology.

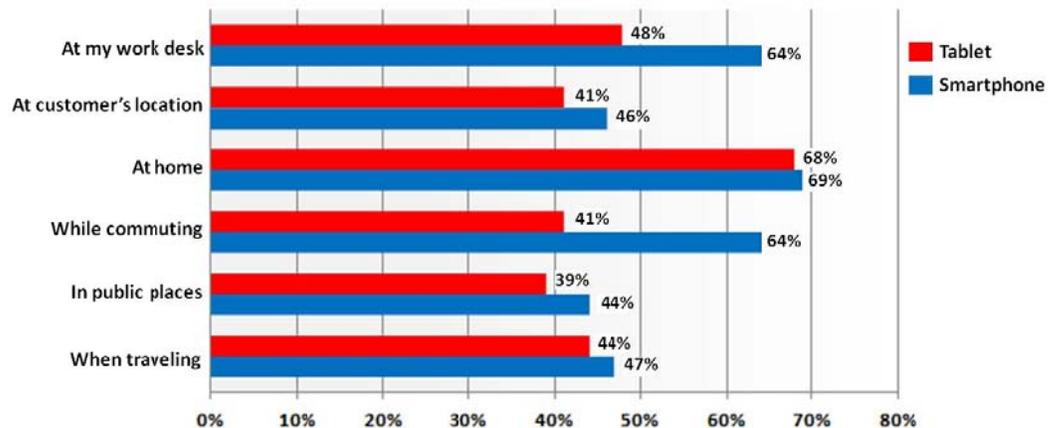
### The bigger picture: *the number of mobility-enabled workers continues to grow*

Despite the clear involvement of technology, BYOD is not just an IT trend, but reflects a much broader change in the way people work and communicate. Noted market analyst *Forrester Research* recently completed a comprehensive study (over 9,000 participants) of changing work styles and concluded that highly mobile knowledge workers now make up about a third of the workforce.

As the chart on the right clearly shows, these 'anywhere, anytime' workers are very much on the move, and so are their communication devices.

For those who may hope that BYOD passes quietly without the need for management action, think again. Given that the number of tablets is expected to triple by 2017, there's every indication that BYOD will remain a hot topic for some time to come.

Where Do You Conduct Business With Your Smartphone or Tablet?



### BYOD do's and don'ts

One of the things that has become very apparent as we've worked with many businesses on their mobile device strategies and implementations is that when it comes to BYOD, *one size does not fit all*. In actuality, an effective approach to BYOD is likely to vary considerably from business to business, and will span a diversity of devices, capabilities and policies.

If we look at the potential ways to address employee use of personal devices in the workplace, there are really three main ways that management can respond:

- 1) Look the other way
- 2) Identify and punish
- 3) Look for the Win-Win

A number of studies have shown that prior to formally addressing BYOD, a fair percentage (around 40%) of business leaders report that they were less-than-fully aware of the extent to which non-sanctioned devices were being used in their companies. Regardless of whether this lack of awareness stems from inattention or purposeful avoidance, the fact is that employee use of personal devices is widespread and growing, and a hands-off approach to BYOD is not likely to bring about an optimum business outcome.

On the other end of the spectrum, most companies that have pursued a punitive approach of threatening or punishing BYOD offenders have ultimately concluded that a different approach would have been more effective. In addition to the strong potential for eroding employee relations, it's likely that a 'drop the hammer' approach will simply shift some percentage of BYOD behavior into the clandestine zone. Interestingly, when *Deloitte Consulting* surveyed the BYOD attitudes of Millennial employees, they found that more than half of the respondents viewed BYOD as an entitlement rather than a privilege, with 30% indicating that they would make a point of finding ways to circumvent any penalty-oriented BYOD policies.

Our experience with clients has clearly shown that the third approach -- the development of a well-thought-through and executed plan that emphasizes the mutual benefits to the business as well as the employees -- is the approach most likely to deliver the best overall results.

### An essential foundation for your BYOD approach

Unsure where to start? The good news is that you don't need to do this alone. While responsibility for BYOD ultimately rests with leadership, the most successful approaches to device management generally involve a multi-disciplinary team. Essential personnel should include the business unit, IT, HR and Legal groups since all of their perspectives will be needed to evaluate key policies such as employee eligibility, expense reimbursement and IT support, as well as important requirements for employee privacy, information security and regulatory compliance.

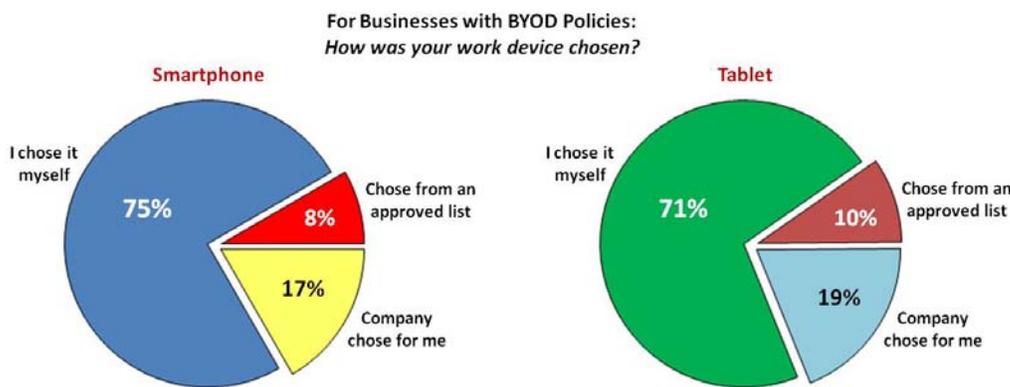
This working group must also include end users. Having the direct input of knowledge workers is essential to uncover and document which mobile devices and applications are really needed to get work done. Consider employing a general employee survey to get a broad base of input. The bottom line: your BYOD policies should be fact-based and not guess work. This is essential for an approach that makes a positive contribution to your business objectives and results.

### The current state of BYOD

When we issued our first Spotlight on mobile devices back in 2012, the market was still largely undecided on how to best approach BYOD. Since then, many businesses have taken steps toward implementing some type of BYOD policy. Earlier this year, an *Aberdeen Group* study found that an impressive three out of four companies surveyed had a BYOD program in place. Far less impressive were the associated findings that over 60% of those companies had embraced an 'anything goes' approach to employee device selection, and also had generally weak safeguards in place for security and compliance.

The earlier mentioned Forrester study found a similar approach to employee freedom of selection (findings on the left).

Although a 'wide-open' freedom of choice approach to device may strike some as overly permissive, anecdotal evidence suggests that the vast majority of devices selected are mainstream products (overwhelmingly Apple or Android) and would likely have been on a company-chosen list anyway.



### An alternative approach

Although BYOD is all about establishing an effective policy for employee-owned devices, there are, in fact, other business models. The most prominent is probably the so-called *COPE* -- 'Company-Owned, Personally Enabled' approach. With COPE, companies don't sanction personal devices for work purposes, but instead offer employees the ability to choose a company-owned device from an approved list. Businesses we have worked with that have adopted a COPE approach report minimal issues and staff push-back. Employees get their device of choice, and the company gets critical control of information security. Typically, a COPE approach is viewed by all parties as a win-win.

**COPE**

Another positive aspect of COPE is the 'business philosophy' that's typically tied to it. Instead of the 'us vs. them' feeling that often accompanies BYOD policies, COPE emphasizes the positive aspects of mutual benefit, trust and innovation. This approach may not be well-suited for all businesses, but the ones we've had direct involvement with have been very pleased with the results.

Thank you for joining me in our 'first installment' of *BYOD - 2014*. Our next Spotlight will focus:

**Readying Your Network for Mobile Device Diversity**

**Expanding BYOD to Include "Bring Your Own Computer" (BYOC)**

**Building a Realistic BYOD Business Case**

**A Smart Approach to "Mobilizing" Your Legacy Business Applications**

Looking forward to our next time together. If you have any comments or questions, please reach us at [questions@coranet.com](mailto:questions@coranet.com).

*Margaret*