Straight Talk from the Corner Office

CORANET
WE PUT A FACE TO TECHNOLOGY®

www.coranet.com

Spotlight on BYOD – *Bring Your Own Device*

July 2012

Welcome to "Straight Talk", a new way for Coranet to share perspectives on important trends in business communications. For this first spotlight, we'll be looking at a rapidly evolving aspect of business mobility – the trend toward *Bring Your Own Device*, or BYOD.

A Quick Overview

BYOD is closely related to another much-talked-about theme: the *Consumerization of IT*. In a nutshell, the idea behind Consumerization is that the adoption of cutting edge communications technology typically happens fastest on the consumer side of peoples' lives, with the result that many employees wind up wanting to use their familiar personal technology in the work environment – irrespective of whether management or IT has given their formal approval. Essentially, the employee is engaged in solution self-provisioning and completely bypassing IT and existing policies and controls in the process.

Although personal smartphones, tablets and laptops are the most prominent forms of Consumerization (hence the more common reference to *Bring Your Own Device*), in fact, many employees are also running unapproved consumer-grade *software applications* on their at-work mobile devices, as well as using these devices to access unauthorized web-based *services* such as cloud storage and social networking sites.

A Situation You Cannot Afford to Ignore

Why is the use of personal devices, applications and services in the workplace an important issue for business leaders?

Top of the list is the need to ensure the protection of company information and intellectual assets. Unlike enterprise-grade solutions that incorporate rigorous security protocols and safeguards as a given, many consumer devices and software applications are seriously lacking in this regard. As a (fairly common) worse case, employees can inadvertently introduce threats into the company network from downloaded freeware and shareware that is purposely infected to compromise remote access mechanisms, steal business information or interfere with company operations. Definitely a situation you want to avoid.

Security is not the only issue when it comes to BYOD. Decisions must also be made in the areas of technical and financial support. If employees are free to use whatever mobile device they want, will some personal devices and operating systems be supported by IT while others will not? If your staff has traditionally received company-provided mobile devices and usage, will employees now receive some financial consideration for their personal devices and associated voice/data plans?

Although security, technical and financial support issues are the norm for any business confronted with BYOD, those companies operating under regulatory requirements are likely to face additional expectations or restrictions when it comes to allowing the use of personal devices and applications. If your business must conform to mandates such as HIPAA, FISMA or PCI DSS, be sure to get expert guidance before deciding on a specific *Bring Your Own Device* approach.

Clearly, BYOD is something that more and more businesses are encountering. The findings of a recent survey of 750 IT professionals (conducted by network management vendor Dell KACE) track with our own observations. For the businesses in the survey that were *not* using iPhones and iPads as their company-issued technology, nearly 60 percent of them reported that their employees were increasingly vocal that the company should provide support for their Apple devices and Mac operating system.

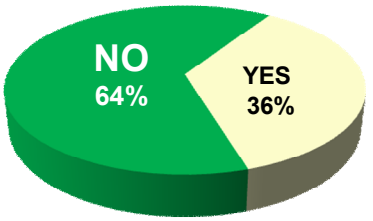
As opposed to a "just say no" stance on one end, or an "anything goes" approach on the other, we have seen a number of customers make the decision to *provide support* for employee-supplied devices – *but with specific restrictions*. As an example, technology giant IBM was recently in the news when they made a company-wide decision to allow employees to use iPhones, but only if the popular Siri voice interface was deactivated (due to security concerns). As an additional condition, any employee wanting to use their personal iPhone must give IBM permission to conduct a remote memory erasure if a security lapse is suspected.

Bring Your Own Device as a New Business Reality

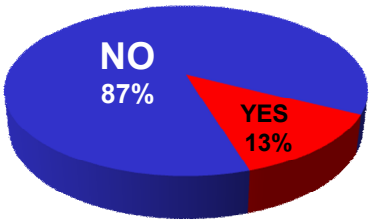
While it may be tempting to view the use of personal devices and applications as a passing fad that requires no action on the part of management, our view (and the general consensus of technology experts) is that Consumerization and BYOD are here to stay. In a May 2012 interview, IBM's Chief Technology Officer succinctly described the reality of employee-provided technology with the remark "*The genie is out of the bottle.*"

This no-turning-back view was also clearly seen in the Dell KACE survey, with the majority of participants seeing BYOB as a serious business issue.

Does your business know what personal devices and applications are being used to interact with the company network?



Is your business currently able to protect company data when personal devices and applications are used by employees?



Our Recommendation

No one likes to be pressured or threatened, but instead of resisting or outright denying employee use of personal technology, we suggest a proactive approach to manage the situation and structure BYOD into a win-win outcome. As your overall goal, you will want to *develop*, *communicate*, and then *enforce* a formal (and clear) policy for use of personal technology with an operational emphasis on *protecting* your company data and infrastructure.

Fortunately, you will not have to start completely from scratch. In terms of policy development, a number of proven best practices already exist that can help you fast-track an *effective and implementable* approach to BYOD that strikes the right balance between employee freedom and company control.

An audit of your wired and wireless infrastructure and devices is a smart place to start. This will identify areas of existing strength and weakness in key areas such as user authentication, data encryption, remote access security and intrusion protection. The findings from the audit will prove very helpful in crafting your company policy as well as identifying what tools the IT team will need going forward.

Once your network has been assessed and any vulnerabilities corrected, your IT personnel will likely need a *mobile device management* toolset that will perform a variety of important functions. Available in both off-the-shelf and customizable versions, these software tools will give you visibility into device-level activity, including the presence of unauthorized users, "rogue" devices that have been compromised, and the use of blacklisted applications. Some of these tools also allow for the ability to "lock and wipe" mobile devices remotely.

Once your policy and tools are in place, consistent IT engagement and visibility will be important for on-going success. To further reinforce management's commitment to BYOD, you may want to consider authorizing small scale pilots to evaluate the issues and do-ability of including new forms of consumerized technology that are brought forward by your employees. Clearly, having management and your IT personnel perceived as supportive and helpful will go far to keeping you aware of how personal technology is actually being used in your business.

Thank you for joining me in this look at the challenges of Consumerization and BYOD. I welcome you sharing your reactions, questions and experiences, as well as suggestions for other topics you would like to see covered.

If you have any questions, please reach us at questions@coranet.com.

Margaret