Transitioning to the New World of BYOD

Brandon Lemke
Technical Sales Consultant

The use of workforce user devices has mushroomed (often 3x) and the complexity of ownership, standards, security and manageability has become very complicated.

The last few years have brought significant changes to workforce computing. Mobile devices are transforming the world of end-user-computing, turning the standards of agency issued desktop computers and laptops upside down.

For most agencies, the road to mobile devices in the workplace began with a few employees buying their own smartphones. They would select the voice and data plans of their choosing and then expense the cost of the service and sometimes the cost of the smartphone to the agency through a departmental budget. IT often tolerated the devices, but support was often left to the employee and the service provider from which the device was purchased.

Now, the use of workforce user devices has mushroomed (often 3x) and the complexity of ownership, standards, security and manageability has become very complicated. Beyond the technology aspect, there are new challenges that need to be addressed with the inherent environment caused by BYOD (bring your own device) policies. With employee owned devices the sensitivity of personal ownership, personal data and personal use of their devices crosses new boundaries outside of the workplace and into the personal lives of employees.

Development and Enforcement of Mobile Polices is a Balancing Act

The challenge of creating polices that balance security and productivity, while weighing the privacy needs of employees when it's their personal device is uncharted territory for many agencies and if not addressed correctly can cause significant contention within an organization.

A recent presentation from Info-Tech Research titled "Transition to BYOD…and Beyond," highlights the following considerations when walking that fine line of agency and private environments.

1. **Understand the differences between personal and organizational data.**
   - The defining feature of BYOD is the fact that devices are used for work, yet personally owned. It is inevitable, therefore, that both organizational data and personal data will be on the same device.
   - Organizational data is defined here as any data used for work. It is not necessarily sensitive data, but can be.
   - Personal data is defined as any data that is not created or used in the context of work. It is not necessarily private or embarrassing, but can be. The challenge is the same for organizational data as it is for personal data: keep the data accessible only by people who should access it.

Continued on back »

WP109420REVA022014

2. Get to know how document containers keep organizational data separate from personal.

- Providing access to agency documents is a particular challenge in a BYOD-friendly organization, because:
- Agency documents can be accessed on personal devices, decreasing control over that information.
- BYOD often necessitates accessing data from a variety of devices, so documents need to be securely accessible from more than one device. Provide a secure document solution that keeps agency documents in their own place, separate from personal documents. Users will be less likely to use insecure methods if there is a securealternative in place.

3. Grasp the importance and limits of selective wipe.

- Remote wipe is an essential security tool. If all else fails, a device can always be erased of all its data, protecting sensitive data that may have been on it. Selective wipe takes this a step further by only erasing sensitive data.
- Selective wipe is not perfect. It is nearly impossible to keep the types of data separate, even with a sandbox approach. Selective wipe will miss some agency data, and even a full remote wipe can only catch some of users' increasingly widely distributed data.

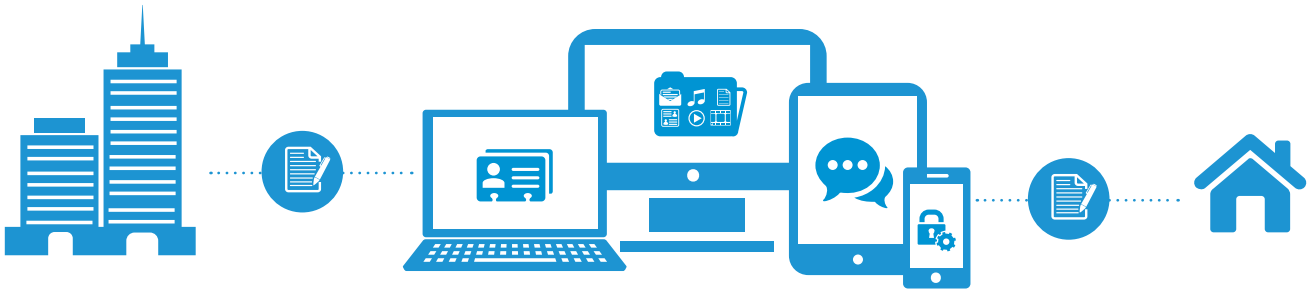
4. Hold your employee's privacy as a priority.

- User trust is critical because no approach is fool-proof. Any method of exerting control or separating data will have a way around it. Anybody can still write down agency secrets using good old pen and paper.
- With data moving to the personal cloud, you no longer know where data goes, and the boundary between personal and agency is even fuzzier.
- Trust your users. If you can't, limit personal devices where possible, but it is still a BYOD world, so prepare for the increased risk of business mixing with personal.

How PCMG can help!

With the explosive demand for enterprise mobility solutions, PCMG stands at the forefront of Managed Solutions. Offering a holistic and secure solution providing end-to-end systems support, PCMG can dramatically increase productivity while lowering costs. With workforce solutions oriented around user success and significant reductions on the IT staff, we reduce the TCO (Total Cost of Ownership) while producing a true solution.

The selection of services covers the entire mobility process from predeployment planning through device management and on to lifecycle management. The entire process is managed and maintained wholly within PCMG as a true single-source provider. With more than twenty years experience and dedicated processes, the PCMG experience is the top of the game. ■



Available from http://www.infotech.com/research/ss/it-transition-to-byod-and-beyond

WP109420REVA022014