5 Rules for Survival in the "Bring Your Own Device" (BYOD) Era

Sponsored by:

BYOD is here to stay for one simple reason: employees don't think that going to work should be a "downgrade" from the tools and devices they use at home to get things done. But supporting BYOD is just a starting point for a whole range of services and capabilities that IT departments around the world can support as they nurture new applications that make network reliability, security and performance paramount.

January 2013

Dan Miller, Senior Analyst – Conversational Commerce

Opus Research, Inc.
350 Brannan St., Suite 340
San Francisco, CA 94107

For sales inquires please e-mail info@opusresearch.net or call +1(415) 904-7666

This report shall be used solely for internal information purposes. Reproduction of this report without prior written permission is forbidden. Access to this report is limited to the license terms agreed to originally and any changes must be agreed upon in writing. The information contained herein has been obtained from sources believe to be reliable. However, Opus Research, Inc. accepts no responsibility whatsoever for the content or legality of the report. Opus Research, Inc. disclaims all warranties as to the accuracy, completeness or adequacy of such information. Further, Opus Research, Inc. shall have no liability for errors, omissions or inadequacies in the information contained herein or interpretations thereof. The opinions expressed herein may not necessarily coincide with the opinions and viewpoints of Opus Research, Inc. and are subject to change without notice.

Five To Survive

Gone are the days when IT managers could mandate what mobile devices meet the strictures of an "approved" list. Instead, a new set of rules (discussed in this document) apply to the world of BYOD. They lay the foundation for employee communications and collaboration across geographical boundaries, time zones and traditional "silos":

- **Rule One: Recognize that everyone has a better mousetrap** – Mobile devices, like smartphones and tablets, are a "considered purchase." They are highly personalized and vital to the individuals that buy them. They are also becoming more and more affordable.

- **Rule Two: Make it easy to discover and add functions** – Think of each device as a gateway to enterprise resources to boost individual productivity, communications, and collaboration, but recognize that you'll be asking Mobile Device Management (MDM) resources to do a lot of heavy lifting in terms of keeping applications up-to-date, secure and compatible.

- **Rule Three: Use "Big Data" and "Analytics" to get Predictive** – Personal data and metadata (concept tagging, etc.) are natural by-products of employee collaboration. They can be used to make diverse workgroups and individuals more productive and more "in control" of the projects they are undertaking through their mobile devices.

- **Rule Four: Balance security and convenience** – Each device has its own distinctive characteristics and attributes. These determine the threat level they pose to enterprise network integrity. IT experts recommend a tri-partite approach: some devices are approved "Platform" devices that are fully supported; others are supported at the "Application" but not device level; and the last group is supported on a fee-based, charge-back basis.

- **Rule Five: Bullet-proof the underlying networks** – As employees discover and define new use cases and applications for mobile interactions, their expectations are for a single network to flat-out work without interruptions or latencies. That means network assurance is crucial not only between and among mobile devices, but also among the back-office systems and databases that are invoked during the course of person-to-person interactions.

For a Copy of the Full Report, Contact Pete Headrick:

pheadrick@opusresearch.net 415.904.7666