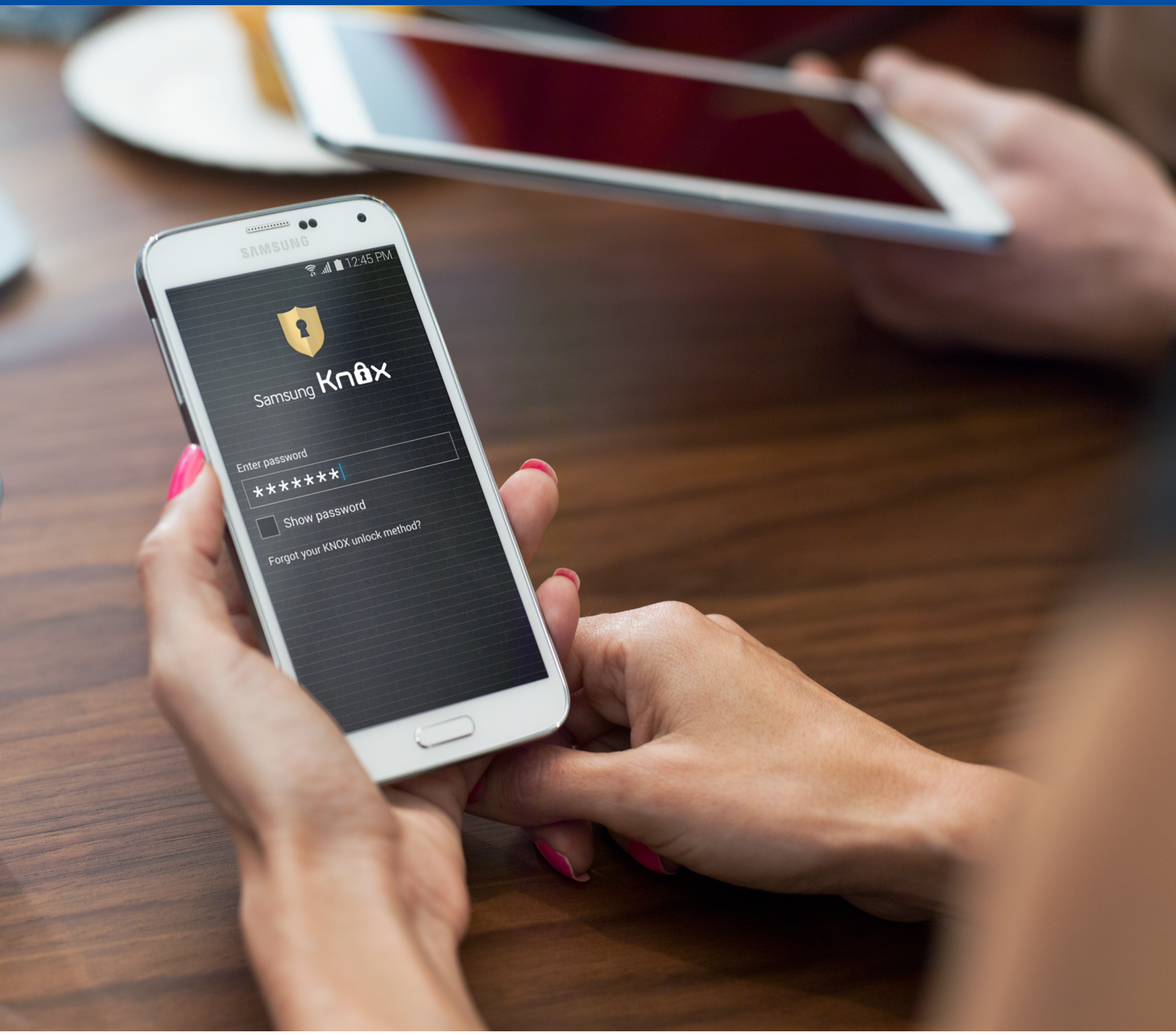


Supporting BYOD Without Reservation: Are We There Yet?

Survey of IT pros explores security fears that may limit BYOD benefits

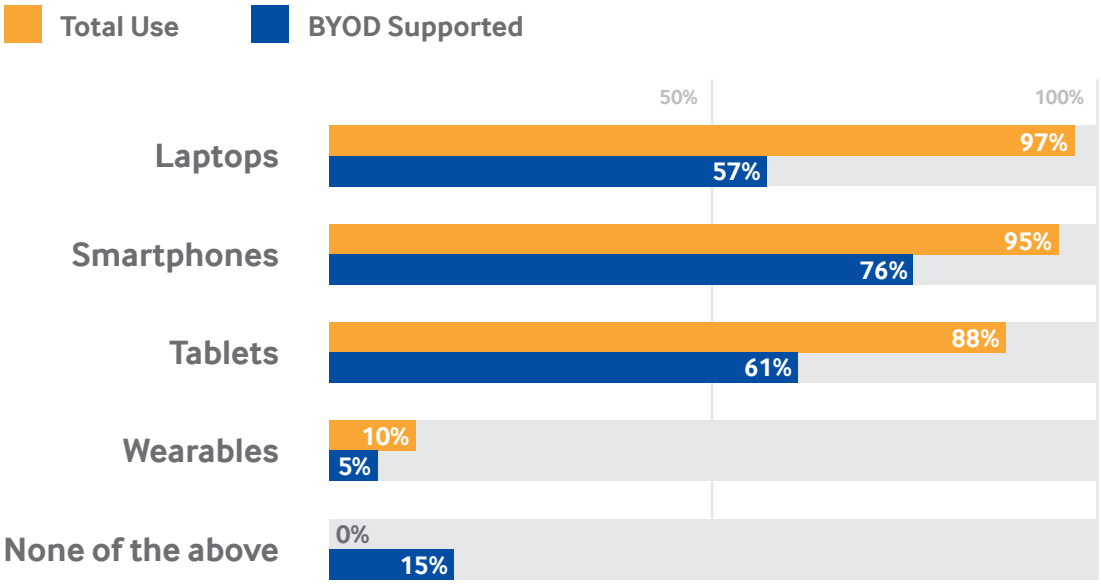
SAMSUNG
BUSINESS

Table of contents

Introduction

In just a few short years, Bring Your Own Device (BYOD) has evolved from a less-than-welcome trend for many businesses to a company-sanctioned everyday reality.[1] The majority (85%) of IT pros responding to a recent survey by Spiceworks indicate their organizations support BYOD devices. This broad acceptance should come as no surprise, given the benefits that have emerged from BYOD – everything from higher employee productivity and lower IT costs[2] to improved business continuity.[3]

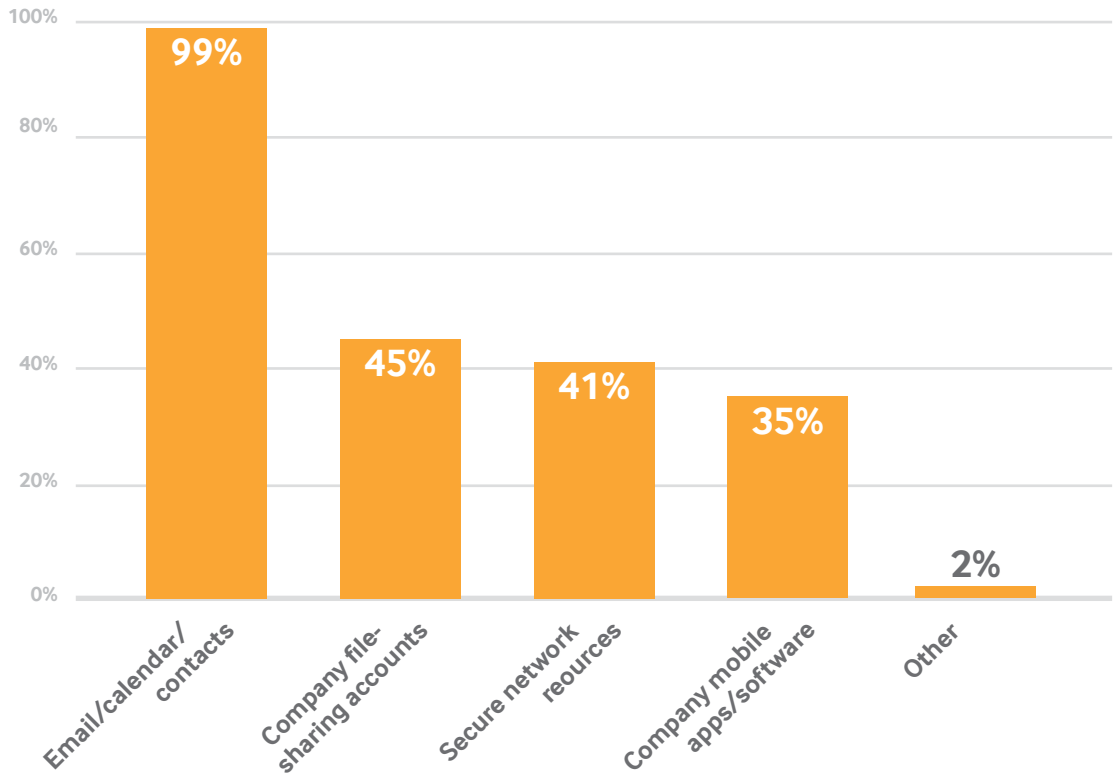
BYOD Device Support



Not surprisingly, the top three employee-owned devices supported by survey respondents are smartphones, tablets and laptops.

What may be surprising, however, is that even though organizations in the survey widely accept BYOD, 86% limit access to a handful of everyday office applications – and only 14% allow full access to corporate assets. For this reason, the benefits they enjoy may also be limited.

BYOD Access to Corporate Assets



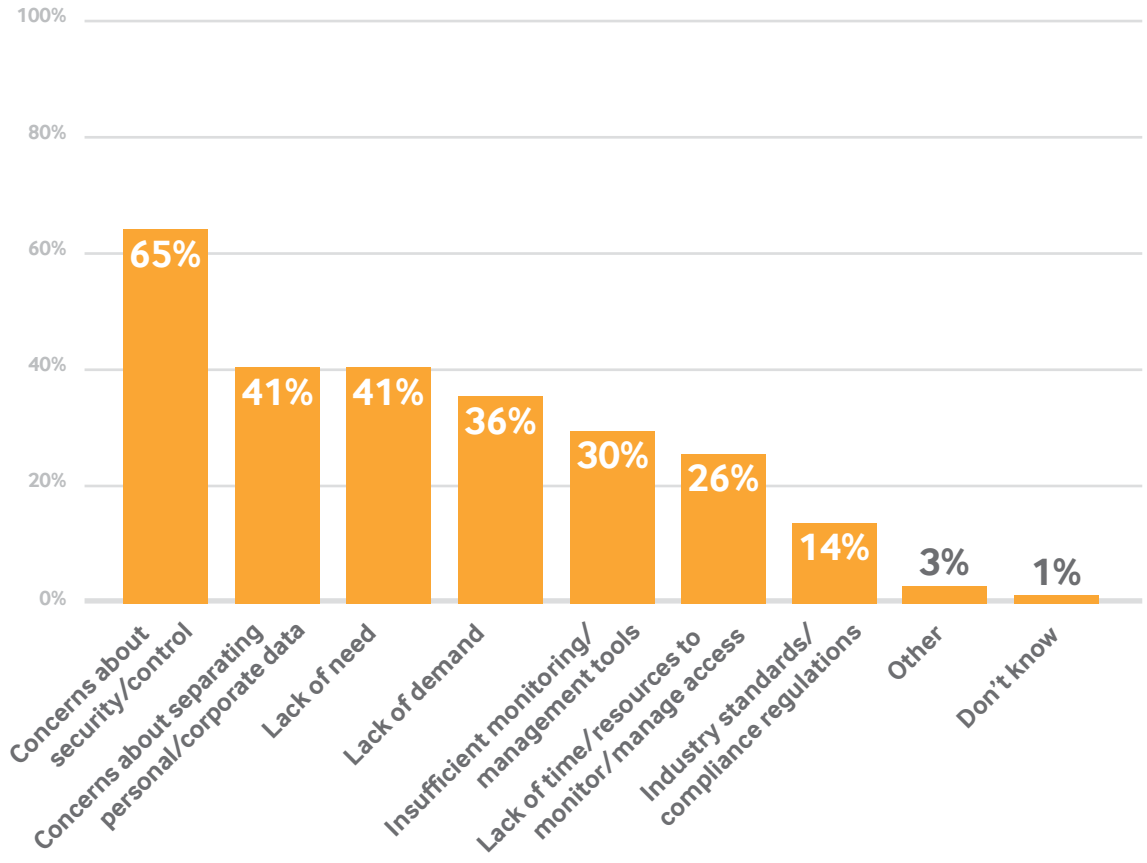
This white paper looks at the concerns that lead organizations to limit BYOD access to corporate assets and at what might alleviate those concerns. It proposes an approach to addressing specific challenges that could pave the way for organizations to support BYOD more broadly – and thereby derive greater benefits from it.

The majority (85%) of IT pros responding to a recent survey by Spiceworks indicate their organizations support BYOD devices.

Security: The greatest BYOD concern

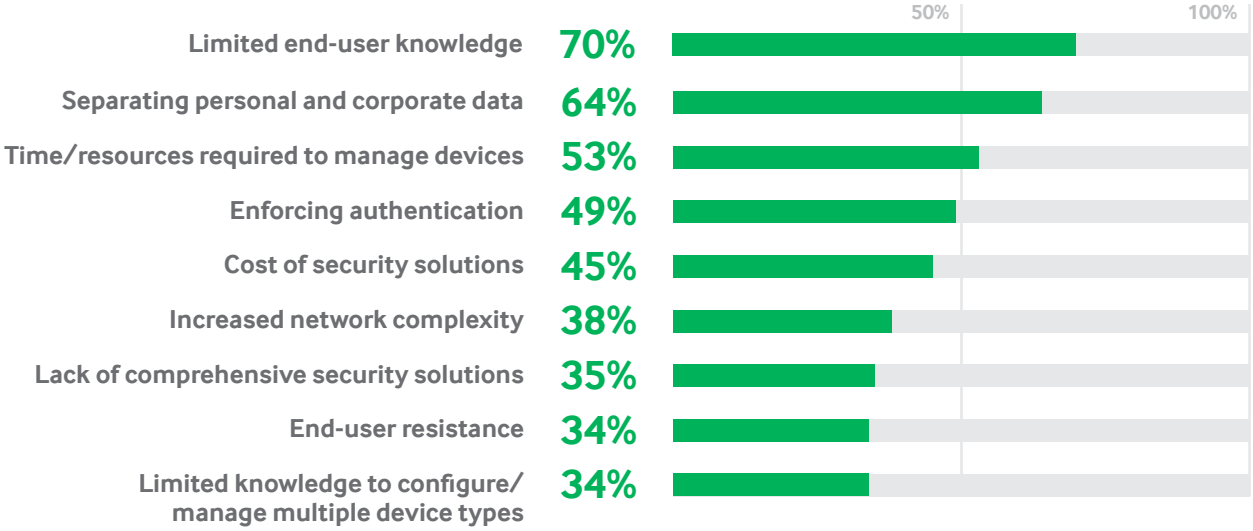
When Spiceworks asked survey participants who restricted BYOD access why they did so, the top answer by a substantial margin was concern about security, followed by concern about keeping personal and corporate data separate. This is consistent with other reports about BYOD concerns over the last several years. "CIOs hesitate to allow full BYOD access because they're balancing convenience and flexibility for employees with security and logistical concerns of their employers," says one industry observer.[4] More recently, *Computerworld* reported on some tricky IT issues that can arise when employees' personal data starts presenting security issues, such as malware that comes in from non-work websites that employees have visited via personal device.[5]

Reasons for Restricted Access
(asked of those *not* allowing full BYOD access)



When asked about the greatest challenge associated with securing access for BYOD, 70% of survey respondents – including both those supporting and not supporting BYOD – cited limited end-user knowledge about risk and security practices.

Top Challenges with Securing Access for BYOD
(asked of those supporting and *not* supporting BYOD)



"CIOs hesitate to allow full BYOD access because they're balancing convenience and flexibility for employees with security and logistical concerns of their employers."

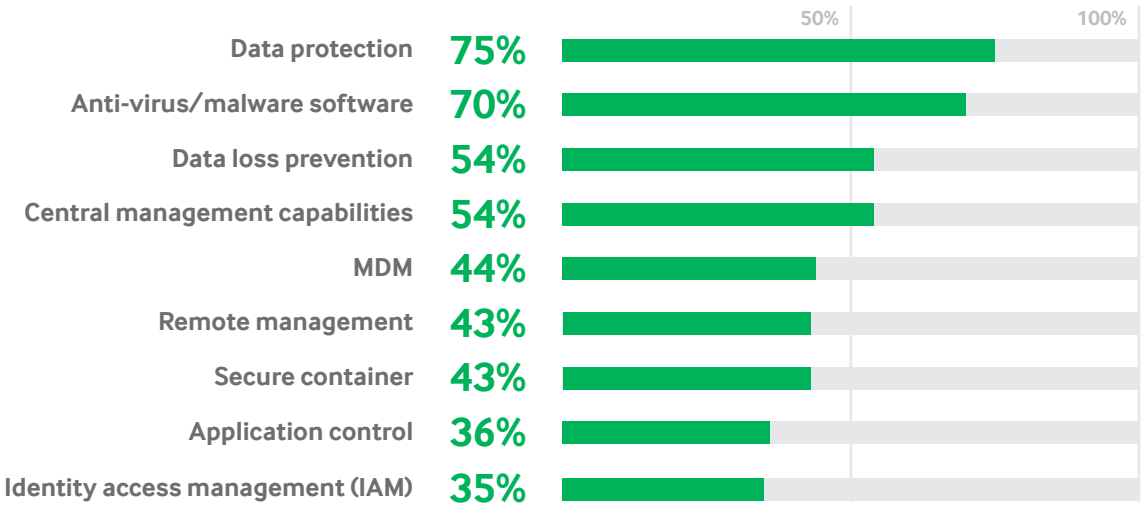
—Computerworld

Securing BYOD: Effective steps IT pros can take

What can be done to make BYOD secure enough that organizations will feel free to allow employees BYOD access to file sharing, network resources, and other critical applications and capabilities? Expert recommendations include clearly establishing policies for how devices can be used and educating employees to be sure they know about, understand and follow those policies.[6] Mobile device management (MDM) is also recommended, as it provides IT with the tools to monitor employee devices and ensure they're being used according to policy.[7]

But is this enough? These steps are important, but none of them – not even MDM – can provide a full measure of mobile security. While more comprehensive mobile security technology solutions are emerging to address the gap, what does IT need to see in these solutions? When asked what factors they considered most important in a BYOD security solution, survey respondents most frequently mentioned data protection and anti-virus/malware software.

Important Factors in a BYOD Security Solution



Comprehensive mobility management solution: Knox from Samsung

Samsung Knox™ is a complete enterprise mobile solution that addresses all the top security concerns IT pros report in the Spiceworks survey. Designed to enhance security of the open-source Android platform, it provides hardware-level, OS-level and application-level security to safeguard corporate data accessed on personal devices. With Knox, employees can use a single device for both personal and business use without compromising business data security. Knox features include:

- Comprehensive protection against malware attacks and hacking
- Multi-layered protection with biometric authentication for authorized device access
- A complete set of cloud-based MDM, IAM and security services that work across device platforms and enable single sign-on or mobile apps
- Remote device/application control through an IT admin or U.S.er portal
- Enhanced application sandbox to secure enterprise apps and prevent data leakage
- Best-in-class device management with more than 390 IT policies
- Compatible with existing enterprise infrastructure

With a multi-layered security model and industry-leading device management capabilities, Knox meets the needs of even the most demanding business environments.

Learn more about Samsung Knox.

With a multi-layered security model and industry-leading device management capabilities, Knox meets the needs of even the most demanding business environments.

About Samsung Business

As a global leader in enterprise mobility and information technology, Samsung Business provides a diverse portfolio of enterprise technologies including smartphones, wearables, tablets, digital displays, hospitality TVs, printers and medical diagnostic equipment. We are committed to putting the business customer at the core of everything we do by delivering comprehensive products, solutions and services across diverse industries including retail, healthcare, hospitality, education and government. For more information, please visit samsung.com/business or follow Samsung Business via Twitter @SamsungBizUSA.

About the survey

Samsung commissioned Spiceworks to conduct an online survey in November 2014 to profile current BYOD practices and pain points. A total of 173 interviews were collected from IT pros in the U.S. Forty-nine percent of the respondents came from organizations with fewer than 100 employees. Another 37% came from organizations with 100 to 499 employees, and 14% came from organizations with 500 or more employees.

SAMSUNG
BUSINESS

Sources

[1] "Celebrating Five Years of BYOD With a Look Back," *Wired Innovation Insights*, December 2014.
http://insights.wired.com/profiles/blogs/celebrating-five-years-of-byod-with-a-look-back#axzz3LovxsSgj

[2] "BYOD All About Benefits and Risks," *Wired Innovation Insights*, September 2013.
http://insights.wired.com/profiles/blogs/bring-your-own-device-benefits-and-risks#axzz3LovxsSgj

[3] "The Impact of BYOD on Business Continuity," *Tech Cocktail*, November 2014.
http://venturebeat.com/2013/03/05/small-businesses-not-huge-companies-will-lead-the-way-for-tablet-growth/

[4] "Why will IT STILL not support BYOD?" *IT World*, May 2012.
http://www.itworld.com/article/2726388/mobile/why-will-it-still-not-support-byod-.html

[5] "Tech support's NSFW problem," *Computerworld*, October 2014.
http://www.computerworld.com/article/2839235/tech-support-s-nsfw-problem.html

[6] "Dos and Don'ts of BYOD," *PC*, October 2014.
http://www.pcmag.com/article2/0,2817,2470068,00.asp

[7] "Keeping BYOD in Check: How to Enforce BYOD Policy," *CIO*, September 2014.
http://www.enterprisecioforum.com/en/blogs/ricknotsodelgadogmailcom/keeping-byod-check-how-enforce-byod-poli