



Supply Chain Operations & Technologies  
 Supply Chain Vendor Compliance  
 Fraud Detection & Reduction  
 Good Governance  
 Turnaround Help

Since January 1996

Based on a sideline story in the October 1, 2014 edition of CIO magazine, the Bring Your Own Device (BYOD) movement, which was all the rage for a while, may be fading to a bit of obscurity.

According to a CompTIA survey of 400 IT and business executives, 51% of respondents from large companies are not engaged in BYOD at all.

The article states that while BYOD was supposed to save companies a lot of money over having to purchase devices for employees and maintain data plans, the concept is fraught with problems such as expense reporting and device management for laptops, tablets, and smartphones: a real myriad of devices running different operating systems and versions.

BYOD was supposed to enable employees to be more productive, allowing employees to work off-hours, but CompTIA's survey revealed that less than half of the companies that offer BYOD believe it boosts productivity in the workforce. BYOD was also supposed to make for a happier employee, but the legalese of BYOD user policies favoring the employer's right to monitor the device's use and to the data on the device have alienated many employees from wanting to voluntarily participate in BYOD programs.

In CIO magazine's November 1, 2014 issue the subject of smartphone kill switches is reviewed. Law enforcement is in favor of this technology as it may reduce crime such as the theft of phones later sold on the secondhand market. A study by William Duckworth, a professor at Creighton University, reveals that 99% of smartphone owners support a kill switch which would disable the phone and could optionally delete all the data. The study informs consumers could save \$3.4B per year in unnecessary replacement costs and insurance fees possibly because – while this direct link is too early to tell – the number of crimes would be decreased.

Even with a kill switch feature, BYOD is still heavily dependent upon usage rules and corporate policies, and let's not forget the potential for viruses and hacking. I don't think that a kill switch option will tilt the balance in favor of BYOD. A solid security policy and clear-cut expense reporting will require providing the necessary device hardware to the employee for their business use, and this investment will more than likely result in a variety of savings across the enterprise in the end.

Happy Thanksgiving everyone!

Norman Katz, CFE, CFS, CCS, MOS  
 Katzscan Inc.

Look for the book --> <http://www.gowerpublishing.com/isbn/9781409407324>



Visit our web sites:

<http://www.katzscan.com/>

<http://www.supplychainfraud.com/>

<http://www.vendorcompliance.info/>

<http://www.turnaroundhelp.com/>

<http://www.supplychainsox.com/>

Do you know of a company - maybe your own - suffering from disconnected dots?

[www.disconnecteddots.com](http://www.disconnecteddots.com)

Let's link!

[www.linkedin.com/in/katzscan](http://www.linkedin.com/in/katzscan)

Follow Katzscan on Twitter!

<http://twitter.com/katzscan>

Katzscan is on Facebook!

<http://www.facebook.com/katzscan>