BIZCOMMUNITY

# Security vs productivity: The mobile device management conundrum

By Viesturs Zalaiskalns

9 Sep 2016

Given the significant productivity benefits delivered by mobility, it is unsurprising to note that it is fast becoming a way of life in many organisations. In fact, Gartner predicts that as many as half of all employers will have instituted mandatory bring-your-own-device (BYOD) policies within the next year.

kaboompics via Pixabay

There are many reasons why mobility, and therefore BYOD, is taking off within enterprises. While employees can clearly be more productive in an office environment when using a laptop or PC, being able to utilise a mobile device for the same tasks means they are able to work from anywhere, and at any time.

The dual benefits of flexibility and productivity are driving an increasing number of organisations to encourage the use of personal mobile devices within the workplace. It makes sense, after all, since employees will inevitably be more comfortable using a device they have personally chosen and which they are intimately familiar with.

However, at the same time, such policies create security concerns. Due to this, organisations tend to make use of mobile device management (MDM) measures to keep some form of control over the proliferation of personal mobile devices in the workplace. The real trouble here is that often such policies are too restrictive, as evidenced by the fact that Gartner believes that as many as 20% of enterprise BYOD programmes will fail, due to overly restrictive MDM measures.

It is clear that both enterprises and users are on a steep learning curve in this regard. Organisations are concerned that mobile devices and apps offer a wide range of new entry points for everything from cyber-criminals to viruses. At the same time, users are concerned that companies are trying to limit how they would normally utilise the device. When this happens, they become disinclined to use it in the workplace at all.

## Less strict is better

Perhaps the answer lies in enterprises working more closely with the application developers. After all, any large work-related application – such as an ERP system – would need to have security built into it from the outset. Therefore, it would seem that as long as employees are using apps authorised by the enterprise, security will automatically be taken care of.

Naturally, there remain certain security procedures that will need to be a part of the organisation's security policies. For example, one would need rules governing the use of unsecured networks to access the company database, and a policy around the encryption of data, to name just two. But at least when it comes to the matter of enterprise applications, businesses should already have security built in.

In fact, it is probably better for an enterprise to be too relaxed, rather than too strict, when it comes to MDM. After all, as long as your software and solutions are encrypted, you should be safe regardless. Also, it's important to remember that any app published in an app store already has to meet a certain range of security requirements. On the other hand, if your policies are too strict, you will likely kill the uptake and use of mobile devices, destroy the BYOD culture in your organisation and ultimately the enterprise will suffer the consequences.

Repercussions the enterprise will likely face with a too strict BYOD culture include:

• Unhappy staff members
• Lower productivity
• Less employee agility
• Reduced flexibility
• Lower attractiveness to potential new employees

In choosing which apps to implement, organisations should obviously only consider ones from well-known and respected vendors. Those who already have a strong reputation in the industry and would not risk damaging it by supplying unsecured apps. Furthermore, in the information age there are many ways to check on both the vendor and the actual software, to ensure that the vendor is trustworthy and the software secure.

Enterprises can:

• Take into account user reviews
• Check that the app is capable of working across multiple different devices and operating systems
• Consider how well its future strategy is mapped out by the vendor
• Choose a vendor with a credible industry reputation and experience

In the end, choosing the right application from a well-respected vendor will allow your organisation to obtain the benefits of BYOD without the need to over-manage device security. This will improve the ability of your employees to do their jobs, while at the same time ensuring they are kept happy. And ultimately, happy employees – especially those that are mobile – are extremely productive employees.

## ABOUT THE AUTHOR

Viesturs Zalaiskalns, HansaWorld South Africa Channel Manager