BIZCOMMUNITY

Managing the enterprise mobility trend

By George Kalebaila

2 Nov 2016

With the increase of Bring Your Own Devices (BYOD) in organisations, effective strategies should be put in place to ensure that employees understand mobile device management policies and the organisation benefits from mobilising the workforce. Mobile device management (MDM) policies must provide for a sufficient range of devices and must be amended constantly to ensure they support the latest developments in technology.

FirmBee via Pixabay

Organisations also need to invest more in educating employees on their rights and responsibilities in order to drive employee cooperation. From an employee perspective, a good understanding of corporate policies relating to BYOD will result in more successful implementation rather than an impression that management is trying to spy or monitor activity on employee's device. Every employee that wishes to have access to BYOD programmes also has to give consent or authorisation to avoid infringing their right to privacy.

The ever-changing digital environment is blurring the lines between personal and business identities. The partitioning of personal data from corporate data is no longer enough and MDM policies have to provide flexibility for personal data to be consumed without compromising the security of the organisation. Organisations need to address employee concerns to show that securing employee devices is in both corporate and employee interest, after all.

Finding balance

Companies are responsible for ensuring a balance between user freedom and productivity by enforcing policies that aim to balance user access and security controls. These policies can increase the variety of devices and platforms users can use, while still enforcing enterprise controls to ensure security standards are met. Restrictive policy regimes will alienate employees and reduce compliancy further undermining corporate security.

The policies will also govern what access controls are given to employees while still enabling them to use their devices freely, dependent on their levels of seniority or business functions, to access core company resources. This reduces or contains the risk, ensuring security is better enforced.

BYOD needs to, however, be within the boundaries of acceptable devices and open standard types, which means companies need to avoid solutions or policies that embrace or accepts everything.

While it is clear that IT departments can't stand in the way of BYOD adoption, enterprise mobility management can help organisations achieve a balance through containerisation solutions – being able to separate user data applications from enterprise ones to maintain user experience while enforcing security controls.

Organisations need to put employee interest first and show that corporate policies are first and foremost helping to address employee and consequently securing corporate resources as a result. This is sure to enlist employee support and increase compliancy and secure enterprise mobility environment.

ABOUT THE AUTHOR

George Kalebaila, senior research manager at International Data Corporation sub-Saharan Africa