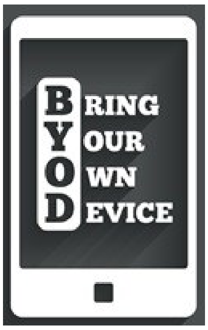
BIZCOMMUNITY

Policies and technologies needed to mitigate the BYOD risk

In the not-too-distant past, companies did not consider the Bring Your Own Device (BYOD) trend to be a threat. These days it's a different story, with companies of all types and sizes realising that BYOD comes hand in hand with many dangers.



blankstock

This is driving the need for policies and technologies to be introduced to mitigate the BYOD risk, says Simon Campbell-Young, CEO of Phoenix Distribution. He says security managers are realising the unsettling implication that they have less and less control of company data, which is being accessed by a plethora of personal devices.

He said that a good BYOD strategy can only be formulated when there is cooperation between the IT department, executives and staff, to decide what works the best, and to ensure that usability, remote working and security are not compromised.

"There are new tools being introduced on a daily basis to ensure mobile data is kept secure. The benefits of mobility are numerous: boosting productivity, allowing working on the go, and users prefer to use their own devices, and don't want the hassle of having to carry a secondary, work device around."

Businesses can't forbid BYOD

He said that businesses cannot forbid BYOD, as this will just see them go underground where the business loses visibility. "This strategy has failed and users will always find a way in. There's a fine line between forbidding and being too permissive where you expose the business to data loss."

This, said Campbell-Young, is where containerisation comes in. "Containerisation separates business and personal assets in the device. The IT department will create and manage containers in each device that give controlled access to various types of data. They can ensure that policy is enforced and any sensitive data encrypted. They can also remotely wipe data off the device in the event it is lost or stolen."

He said that this separation of business and personal assets ensures that employees only need to carry a single device of their choice - and can still make the most of secure access to business data.

"Another useful tool for keeping mobiles safe is mobile device management (MDM) solutions. MDM solutions allow the technical department to keep mobile devices safe across all the disparate operating systems, ensuring secure business communications, remote wiping of business data and automatic device configuration."

These solutions, he explained, also clearly separate business and personal data on mobile devices. "In this way, should a staff member leave the company, or lose his mobile phone, the IT department can wipe all the business data off the device while leaving the personal data untouched. Using these tools ensure that it isn't a case of bring your own danger. They address all the BYOD security issues, while ensuring that staff are not inconvenienced, creating a secure and productive mobile workforce."