The challenge of mobile security for BYOD

Mobile security that complies with the Protection of Personal Information Act (POPI) is going to be particularly challenging for organisations that have embraced BYOD (Bring Your Own Device).

Image: www.freedigitalphotos.net

Companies need to recognise the risk within their firms, as the majority of employees use their personal devices to access corporate information. Organisations need to take the necessary precautions to avoid company data being compromised, while still respecting employees' privacy.

BYOD within firms has changed the traditional security model as a company's IT perimeter can no longer be defined, both in terms of physical location and asset ownership. Devices such as smartphones and tablets are used by employees for both work and personal use and many organisations battle to establish acceptable procedures and support models that balance employees' needs and the company's security concerns.

"With talks about POPI being implemented in the New Year, it's important for companies to take action with regards to protecting their data - especially those that have adopted the BYOD trend," stressed Jeremy Matthews, Country Manager of Panda Security.

Modern and well-founded law

POPI, intends to place restrictions on how companies handle personal data. It is a mechanism that enables people to access and enforce their privacy rights on a day-to-day basis. POPI's principles make it one of South Africa's most modern and well-founded laws - ensuring that effective end-point security and device management is in place will be critical to meeting the terms of the Act.

Practical steps to implement core mobile security:

- Make use of a Mobile Device Management solution enabling centralised administration and control;
- Implement password policy management, forcing users to make use of a complex password/code on their mobile

devices;

- Use remote wiping and locking/unlocking when phones are compromised;
- Use geolocation in case of loss or theft; and
- Keep track of who is doing what and when, through scheduled reports.

All of the above-mentioned features are included in Panda Cloud Systems Management (PCSM) and Panda Cloud Fusion (PCF).

Mobile Device Management solutions can be used for both company-owned and employee-owned devices. By controlling and protecting the data and configuration settings for all mobile devices on a network, Mobile Device Management can reduce support costs and business risks. IT administrators will have tight control over the apps that users can install and execute; such as games, usage of camera or in-app purchases. The intent of Mobile Device Management is to optimise functionality and security of mobile devices, while minimising cost and downtime.

Firms with BYOD policies need to start looking at implementing multiplatform Mobile Device Management as a matter of urgency, as well as applying security frameworks and solutions that permit end-to-end control over the management of data on mobile devices. Ideally, these security procedures need to be auditable so that compliance with POPI can be demonstrated.