ACKNOWLEDGMENT

DR PETER TOBIN is a consultant at IACT-Africa. He can be contacted on 083 922 3444 or petert@iact-africa.com.

Mobile data devices and POPI

If you have a business which uses mobile data devices, POPI will affect you

On 11 April 2014, the government initiated the first steps towards the full implementation of the POPI Act (2013) across South Africa. One aspect that is receiving particular attention is how mobile digital devices capable of storing personal information (PI) and data are deployed.

"South Africa, in common with other countries, has seen an explosive growth in the use of mobile data devices (MDD) in line with the BYOD trend, from smartphones to tablets, all impacted by the need for personal information (PI) protection as demanded by the POPI Act," says Dr Peter Tobin, consultant with IACT-Africa.

"Now that PI is stored on privately-owned devices used for business purposes, the demands placed on the information officer as defined in the POPI Act represent a major challenge and a significant component of the overall risks associated with protection of PI."

Tom Carter, business development manager at iStorage-Africa, has first-hand experience of the value that comes from securing such mobile data devices. "Many of our clients recognise the negative impact that data loss or inadvertent destruction can have on vital business data. That's why the range of secure mobile devices we offer has proved so successful with clients with demanding applications such as military-grade mobile data protection."

Colin McCarthy is MD of Uthanda ICT, a Microsoft partner and managed service provider which offers professional IT support for small to medium sized businesses. He is adamant about the need to treat MDD seriously. "Our company policy clearly states that we will ensure that mobile devices with on-board storage, such as laptops and tablets, need to be encrypted as just one of the steps to secure the data they contain."

"Not only that, we recognise that flash drives (memory sticks) are often ignored or forgotten, and we have evaluated the best way to ensure that devices such as these and other portable back-up devices need the same level of encryption. Uthanda has begun advising its clients about POPI Act compliance as part of their broader approach to adding value in client service delivery," says Eben Müller, IT director at Uthanda.

"We know our clients treat us as trusted advisors, and we are not willing to put our reputation at risk in this key area of data privacy and POPI Act compliance, so what we say is what we do," adds Colin.

From the perspective of one of South Africa's leading growth areas, advocate Louis Nel says POPI is upon us and the entire spectrum of travel, tourism and related industries and their use of MDD are affected.

"Each sector, from the travel agent (face-to-face or online), to the conference organiser, conference venue and accommodation and transport providers, capture personal information addressed by POPI. The entire industry needs to take stock and implement urgent steps to ensure proactive compliance, or face extremely adverse implications ranging from R10-million fines and imprisonment to civil action and publication of IT breaches with concomitant, severe reputational damage."

Digital forensics is another area impacted by the POPI Act. Alan Evan-Hanes, forensic investigator and consultant with Althair, has extensive experience in the implications of poor security practices in the area of MDDs. "My colleagues and I have seen too many cases where regret overwhelms forethought. Too often clients realise too late that a more formal approach, such as the use of encrypted technology, while appearing to be a significant investment in the short-term, actually pays huge dividends very quickly. Just one incident of loss or data breach could destroy a huge amount of value and reputation (hard to build and too easy to destroy) which could easily have been avoided."

Frik Kitching, forensic investigator of CLAMP, says, "Clients need to track MDD movement, for devices such as laptops, tablets and cell phones, not only for the potential physical asset value loss but increasingly because of the value of the data contained in those devices. Our forensic work has taken on an additional dimension now that POPI Act compliance demands organisations take seriously how and where they store personal information, protect it from unauthorised access and recover it intact whenever possible."

Information security and privacy governance mechanisms for MDD also need to be put into place, says John Cato, Information Security and Governance consultant at IACT-Africa. He says that many organisations believe that by implementing technologies such as encryption and data loss prevention they are protected against losing information. While this is true to an extent, good security and privacy governance steps also need to be taken as many information leakages are caused by staff members, either unintentionally or for malicious reasons.

Good governance for MDD starts with building mobile device responsibilities into information security, privacy and BYOD policies. By making staff members aware of their responsibilities for protecting PI (and other company information), the risk of losing information will be reduced as they know they will be held accountable for any information losses.

So what should organisations do about personal information protection on mobile data devices?

"Take minor steps to avoid a major data breach," suggests Dr Tobin. ■

Five tips to avoid a data breach:

- Minimise the amount of PI stored on MDD;
- If you must use an MDD, ensure you know what PI you are storing on your MMD in case it is lost or stolen;
- Notify your information officer as soon as a loss of your MDD with PI occurs;
- Only use an MDD with device encryption for storing PI; and
- Remember to comply with POPI, or suffer the consequences.