Demystifying POPI

The Protection of Personal Information (POPI) Act will be a landmark piece of regulation, once implemented. It clearly describes certain conditions and minimum requirements. But it deals with principles and some guidance may be needed on operational detail.

Financial service providers should already be obtaining consent to collect personal information, limit collection to what is relevant, process data only for a defined purpose, and ensure good data quality.

Power to data subjects

POPI grants certain rights to consumers (which it refers to as data subjects) to object to the processing of personal information and to ask for corrections and deletions to such information. Businesses will have to design processes to deal with such requests, which will be subject to the draft regulations published in September 2017.

Section 19 of the Act provides important clues on what else needs to be done. The phrase appropriate, reasonable technical and organisational measures, implies that judgement is needed in assessing readiness, and that activities span across the whole organisation.

Section 19 also mandates continuous risk management, which should come naturally to financial service providers. Further, it refers to generally accepted information security practices.

Smaller businesses tend to be less formal than large corporations. However, standards such as ISO/IEC 27001 (that deals specifically with information security) can be adapted to the needs of any business.

Good starting points

A good starting point is to take stock of what kind of personal information is held in your business and where it is stored. This could be on your premises or at a third-party site.

By default, the head of an organisation is also that organisation's information officer. This person will in future be answerable to the POPI regulator.

The information officer is also responsible for overall compliance. It follows that information security does not start with technology; it is people who make information security succeed or fail.

Human resources security should include screening of job applicants and procedures for employment termination. Awareness sessions should be held regularly and highlight, for example, the proper use of passwords and the requirement to encrypt sensitive information when sending spreadsheets with personal information over insecure channels such as email.

The private use of business equipment should be minimised to avoid the risks of malware infections and leakage of sensitive information. This can be enforced through an acceptable usage policy and/or technical measures.

Appropriate protection

Under POPI, assets need to be well protected. This includes physical access control and environmental protection against power outages and fire. All PCs and laptops should be encrypted because data in the wrong hands can cause more damage than theft of equipment.

Companies should regularly test the restoring of critical data from encrypted, off-site backups. Do not trust strangers to repair your equipment and ensure that sensitive data cannot be retrieved from scrapped machines or discarded storage media.

Access to data must be well managed according to the principles of need to know and segregation of duties. Further, access rights to systems must be reviewed regularly to respond to joiners, leavers and changed responsibilities.

Sharing is caring

IT service providers have many additional responsibilities, which includes regular vulnerability assessments to ensure that their defences work as intended. Any reputable service provider will gladly share its information security policy, disaster recovery plan, business continuity plan and related documents with relevant parties.

No business is totally immune to the threat of data breaches. An incident management plan can improve resilience and should also address communication with various stakeholders. Business partners may be able to help with advice and practical actions.

How do you know when you have done enough? The answer depends on the circumstances of an individual business, but the above-mentioned actions should provide some guidance to get yourself off on the right foot.

Christoph Fuhrmann
Executive Head: Information Technology
Brolink