The Protection of Personal Information Act No 4 of 2013 ("POPI"): Rethink the 'archi*tech*ture' of your business

by Kellie-Kirsty Hennessy

'Security is a not a product, but a process. It's designing the entire system such that all security measures work together.' - Bruce Schneier

The internal governance of the processing of personal information is of crucial importance. POPI obligates 'responsible parties' to take appropriate, reasonable technical and organisational measures to ensure the safeguarding of the processing of personal information. In relation to the obligations set out in POPI, one is required to carefully scrutinise the current information technology architecture in place or alternatively, to design a carefully moderated system for IT Governance relevant to your unique industry risks.

The POPI Act contains extremely broad definitions regarding 'processing' and 'personal information'. The girth of the Act's operation places an active need for any prudent business owner to establish a framework to manage the integrity of information, as well as to identify the security risks involved. POPI places a mandatory obligation on a 'responsible party' to secure the integrity and confidentiality of personal information in its possession or under its control. As part and parcel of this requirement, POPI necessitates that any person who acts as an information operator in the processing of information must enter into written confidentiality agreements prior to access to personal information. Furthermore, POPI requires a 'responsible party' to take measures to prevent the loss, damage, unauthorised destruction, unlawful access, or unlawful processing of personal information.

It is prophetic for directors of companies to understand the duality of the role of a 'responsible party' in processing personal information lawfully in terms of POPI, as well as the obligations placed on directors by the Companies Act No 71 of 2008 for the appropriate duties of care. Accordingly, a director, or the board of directors, may be held accountable for future breaches of POPI, due to a failure to take reasonable steps in applying appropriate principles of IT Governance to prevent action. Companies are referred to the King III Report on Corporate Governance for South Africa (The Institute of Directors in Southern Africa), which contains a code of practice for governance of information technology. It is suggested that each company or business scrutinise this code and implement the same to design a system which serves to operate in anticipation of the pending data privacy legislation.

As part of the encouraged strategy of identifying reasonably foreseeable internal and external risks, business owners are cautioned to understand the nature of the technology used in any business, as well as the latent information technology capabilities to process personal information. The operation and use of even the most rudimentary office equipment may contain concealed and material security risks. In an astonishing investigative journalism documentary, CBC News revealed that digital copiers contain hard drives similar to those found in a computer which stores an image of every document copied, emailed, faxed or scanned by that machine. The hard drive can be easily removed by any person with access to the machine and the contents may be easily processed with software available free on the internet![1] Companies which rent these machines are vulnerable to the storing of their confidential details and the personal information of their employees, which is haplessly handed over to any subsequent lessee for processing. This also should raise alarm bells to those involved in industries which supply Photostat machines, printers and scanners for use by the public for a fee. The security risk of access and processing of this information will result in violations of the POPI Act and must be addressed.

POPI places the obligation on 'responsible parties' to have due regard to generally accepted information security practices and procedures and to regularly verify that safeguards in place are updated and effective to new advances in technology. Take this opportunity to revaluate your current business and the processing risks involved. Directors are admonished to place an IT governance policy on the agenda for the board and *vis-à-vis* smaller businesses are encouraged to meet with staff to discuss current challenges. The way forward is in developing a strategic plan which successfully defines the information architecture relevant to your business, holistically combining the elements of staff education, technology capacities and information governance which all work together to ensure POPI compliance.

By Kellie Hennesy - Johanette Rheeder Inc.

www.labourmart.co.za / www.jrattorneys.co.za / info@labourmart.co.za

[1] Armen Keteyian, '*Digital Photocopiers Loaded With Secrets*' CBS April 19, 2010

(http://www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets/)