POPI Act crucial component in addressing cybercrime

By Leishen Pillay

27 Jan 2016

If one considers that between 70% and 80% of South African adults have been victims of cybercrime in their lifetime, the Protection of Personal Information (POPI) Act is an essential leap forward in South African legislative terms, as it is the first piece of legislation to specifically address, as its main objective, the protection of personal information.

© weerapat1003 - Fotolia.com

Cybercrime cost the South African economy approximately R5.8 billion in 2014. Addressing the substantial financial impact of cybercrime on South African businesses has been quite critical, especially of late, as the cost and impact of cybercrime continues to escalate almost unabated.

The POPI Act, which was signed into law in November 2013, although not fully implemented, aims to promote the protection of personal information, which falls under the broader Constitutional right to privacy, and introduce minimum requirements to protect personal information, by regulating how such information is processed, stored, secured, and ultimately destroyed.

These minimum requirements are not currently mandatory and could be one of the reasons why cybercrime is on the rise. Access to personal information is fundamental to cyber criminals carrying out cybercrimes and any legislation that attempts to protect the confidentiality of personal information, such as the POPI Act, will definitely assist in reducing cybercrime. The POPI Act is a crucial component in the overall policy framework to address cybercrime.

With a development track over a decade long, the POPI Act has been carefully considered and includes international best practice standards, which will elevate South Africa's data privacy protection to levels that would more readily facilitate economic trade with nations sensitive about data privacy protection, such as members of the European Union.

Once it is fully implemented, businesses will have one year from commencement to comply with the legislation. Whilst this period may be sufficient for smaller businesses, larger enterprises, which may be far more complex, could need as much as two to three years to be fully compliant. Getting a head start with compliance activities could prove invaluable to avoid potential fines and possibly imprisonment.

A failure to comply with the POPI Act could expose businesses to fines from the regulator of up to R10-million or in certain instances of non-compliance, a court sanctioned fine and/or a period of imprisonment of up to 10 years.

Getting ready for implementation

If you have not already started with integrating the POPI Act's requirements into your business, you should consider starting now. Here is how you can get your house in order:

1. Read the POPI Act, and **understand what your responsibilities are**. Businesses should also understand the rights of their customers in terms of the POPI Act, how those rights may be enforced against them, and the consequences of not complying with the reciprocal obligations.
2. **Determine what your current levels of compliance are and the steps necessary for you to comply with the POPI Act.** Amongst other obligations, the POPI Act requires you to take reasonable technological and organisational measures to ensure certain minimum standards are achieved in protecting the integrity and confidentiality of personal information. Ensure that you understand how this translates into your business specifically and budget for any potential changes to your annual budget, as you may be required to make certain technological upgrades, as well as updating existing policies and procedures.
3. If you fail to plan, you plan to fail. **Put a project plan in place**, with measurable deliverables and timelines, to ensure that all the requirements of the POPI Act are addressed before the Act commences. You will need a cradle-to-grave approach, which should address the total life cycle of personal information in your business. Make provision for the actual changes that must be implemented to bring about compliance in your business and then systematically execute and monitor the progress of the project plan.
4. **Review your employee and third party service provider agreements** to ensure that they clearly reflect your obligations in terms of the POPI Act. Their breach may be your problem.
5. **Consider whether your business should purchase cyber liability insurance** to manage the risks associated with a breach of security, or the POPI Act.

If you are in doubt about any aspect of the POPI Act, and what may be required to comply, specialist advice should be sought.

It is crucial that every business familiarise itself with the rights and obligations in the POPI Act to safeguard both its customers and its business interests. Notwithstanding that the POPI Act is not yet fully effective, any compliance activities undertaken now will bring your business closer to compliance with the POPI Act and may prevent your organisation from becoming a victim of cybercrime. It is advisable to put steps in place to prevent cybercrime from occurring, rather than attempting to mitigate the adverse effects once an incident occurs.

ABOUT THE AUTHOR

Leishen Pillay is a partner in the Technology, Telecomms and Media Practice at global law firm, Hogan Lovells.