POPI: the race to data safety

By Gregory Anderson

8 Jun 2015

The passing of the Protection of Personal Information Act (POPI) into South African law in 2013 and the imminent appointment of an information regulator has forced local businesses to sit up and listen as they are given a deadline of a year to comply.

Proclaiming POPI into effect

Relax - the effective date for POPI is not set in stone. POPI became an Act of Parliament in 2013 however, it will only come into effect by proclamation from the president Jacob Zuma in the Government Gazette. So from the date of the President's proclamation, companies - no matter their size - will have one year to make the necessary changes to become POPI compliant.

However, the President has already proclaimed certain sections of POPI into effect, specifically the section that provides for the establishment of an information regulator to oversee and enforce the provisions of POPI. It is suspected that, once said regulator has been established, the president will proclaim the rest of the provisions of POPI into effect. There is currently no clue as to when this date may be, however, it has been predicted that it could be towards the end of this year. Nevertheless, you should already be thinking about - if not implementing - the necessary changes.

Knowing that it is coming is all good and well, but do you know what POPI is and how it affects your business?

Introducing POPI

For argument's sake let's pretend that you been living under a rock and that you have no idea what POPI is. In this case you would need to know that the POPI Act is an all-inclusive piece of legislation which aims to regulate the processing (see the very detailed definition of this word in the Act) of personal information.

POPI outlines personal information as any information relating to an identifiable, living natural or juristic person and includes but is not limited to contact details, demographic information, history, biometric information, opinions of and about a person or private correspondence (like email). Those that fail to comply with POPI in the set-out time-limit - and that don't apply for and receive an extension - may be subjected to fines of up to R10 million and even jail time.

One of the eight conditions established by POPI in order for the processing of personal data to be lawful is that reasonable security measures be applied to protect it. So the short answer to companies that wonder if POPI will affect them is: If you have customers, partners or staff and you have any of their personal information stored in your database then POPI definitely applies to you.

Safeguarding your data

The next logical question then is, how safe is your data?

POPI makes it obligatory for companies to do what IT security vendors have been preaching for years: put the security of data first. Because of POPI local companies will need to better protect and manage the personal records and information they process. This pertains to information of their customers and clients but it also concerns every employee in their service.

Stuart Mles via freedigitalphotos.net

In the technology and information age we live in, POPI can be seen as a starting point for businesses and professionals who want to take stock of how they handle and subsequently govern this valuable business asset. With cybercrime incidents increasing and gaining complexity and trends like Cloud, BYOD as well as the Internet of Everything in full swing, there are a lot of information channels that need to be secured within any organisation's network.

In addition to this information 'stock take', it is a good idea to map out how you - as a company - plan to meet the legal requirements of POPI. This is an especially vital step when it comes to the security of company data. Do you know what security measures you have in place? Do you have in place a holistic security solution that covers you from end-to-end?

Technologies designed to protect

Have your business taken measures toward data loss prevention and encryption in your business? Technologies like Trend Micro Integrated DLP (Data Loss Prevention) protect your company data from endpoint to cloud based on the policies set up on what data can leave the organisation, while encryption technologies like Trend Micro Endpoint Encryption provide full-disk, file encryption and data protection.

Technologies that are designed to protect your business in the cloud and at the virtual layer can protect your company data. Trend Micro Deep Security is a robust solution for cloud computing and virtual environments because it enables the user to take advantage of "better-than-physical" protection. It is a single platform that integrates all security technologies and in turn is able to resolve any operational issues that may arise in the virtual environment.

Trend Micro's Deep Security Solution delivers comprehensive, adaptive, highly efficient, agentless and agent-based protection, including anti-malware, intrusion detection and prevention, firewall, web application protection, integrity monitoring and log inspection. With Deep Security businesses will be aware of security breaches and will have advanced protection for physical, virtual and cloud servers.

The protection of data should have always been a company priority because a data breach not only puts your clients and customers at risk, but it risks the reputation of your entire business. Every person that trusts you with their data, is essentially placing in you a belief that it will be protected and once that information is breached, the trust is gone for good and you will be left in despair as clients and customers turn their backs on your business. Are you willing to risk that?

ABOUT GREGORY ANDERSON

Gregory Anderson is the country manager for Trend Mcro South Africa.

- POPI: the race to data safety - 8 Jun 2015

View my profile and articles...