WERKSMANS
ATTORNEYS

REGULATORY

You have to say something as with data disappearing, your embarrassment will not

1 November 2017 *4 min read*

by Ahmore Burger-Smidt, Head of Data Privacy Practice

The Protection of Personal Information Act, Act 4 of 2013 ("**POPIA**") addresses, amongst others, poor information control and security. Therefore, data which is still required for a specified purpose for which it was collected and is, however, not accessed regularly, should be archived and stored securely.

Information security involves all measures used to protect any information generated by a company or individual, which is not intended to be made publicly available, from compromise, loss of integrity or unavailability. This can be relevant for personal information, security classified information and commercially confidential information.

The largest data leak recorded in South Africa to date and reported on 17 October 2017, has been traced to a Web server registered to a real estate company based in Pretoria. It appears that Jigsaw Holdings ("**Jigsaw**"), a holding company for several real estate franchises, including Realty1, ERA and Aida is the party responsible for allowing the data breach to take place. It has been reported that "Whois lookup" a poorly configured website, had exceptionally lax security and until recently allowed anyone with limited technical knowledge to view or download any of the 75 million database records it held. More than 31 million of those records consisted of the personal data of South African citizens and these 31 million records which contain personal information of South African citizens are now in the public domain.

According to a report of TechCentral on 19 October 2017, TechCentral contacted Jigsaw for comment during the morning of Wednesday, 18 October 2017, and Jigsaw management requested time to investigate the issue. By Wednesday evening of the same day, neither the company nor its legal counsel was contactable.

In this instance, the ignorance as to security awareness, is glaring.

Personal information security specifically relates to companies taking reasonable steps to protect personal information in their possession. Personal information security measures should be designed with the aim to prevent misuse, interference, loss or unauthorised accessing, modification or disclosure of personal information. Furthermore, security measures should be in place to detect privacy breaches promptly, in order to respond to potential privacy breaches in a timely and appropriate manner.

South Africa and Brazil, where physical crimes are among the highest in the world, are both clearly emerging as countries with high levels of cybercrime. South Africa, China and Singapore are also countries with high levels of free anti-virus software users with the associated risk of large numbers of people accessing the internet and becoming cybercrime victims via mobile devices. Free anti-virus software is not necessarily safe and secure since these software programmes are often targeted by cybercriminals to 'hide' malware inside the free software that often 'pops-up' unsolicited on mobile devices.

In 2016, the FBI had listed South Africa as globally the 12th most active country in terms of the occurrence of cybercrime.

WHAT SHOULD COMPANIES DO?

Companies should consider in detail the risk of disasters and the business impacts of such occurrences. Furthermore, companies should design preventative and reactive controls. When disasters strike, confidential, secret, personally identifiable or sensitive data may be exposed, and business continuity plans must take into account how to protect information, reputation and assets.

When a breach has occurred, the company should ideally openly and timeously communicate with the customers, stating the nature of the breach. Companies should clarify what information has been stolen and what the customer can do to ensure that it is not a victim of identity theft. Importantly, tell the story – what the company is doing to prevent future data breaches, e.g., improving physical security in the event that computers have been stolen or improving the quality of security software.

With the full commencement of POPIA, it is recommended that companies establish a comprehensive breach plan and ensure that all employees know what steps to take in the event of a breach! Security breaches must be planned for.

Companies and management should not disappear with lost data. Be pro active, understand, plan and correct.

POPIA has not been fully implemented and we all expect this to take place early in 2018. In terms of POPIA, a negligent company could be liable for up to R10 million in fines and negligent company officers jailed for up to 10 years.

Download



Ahmore Burger-Smidt

Head of Regulatory

View Profile