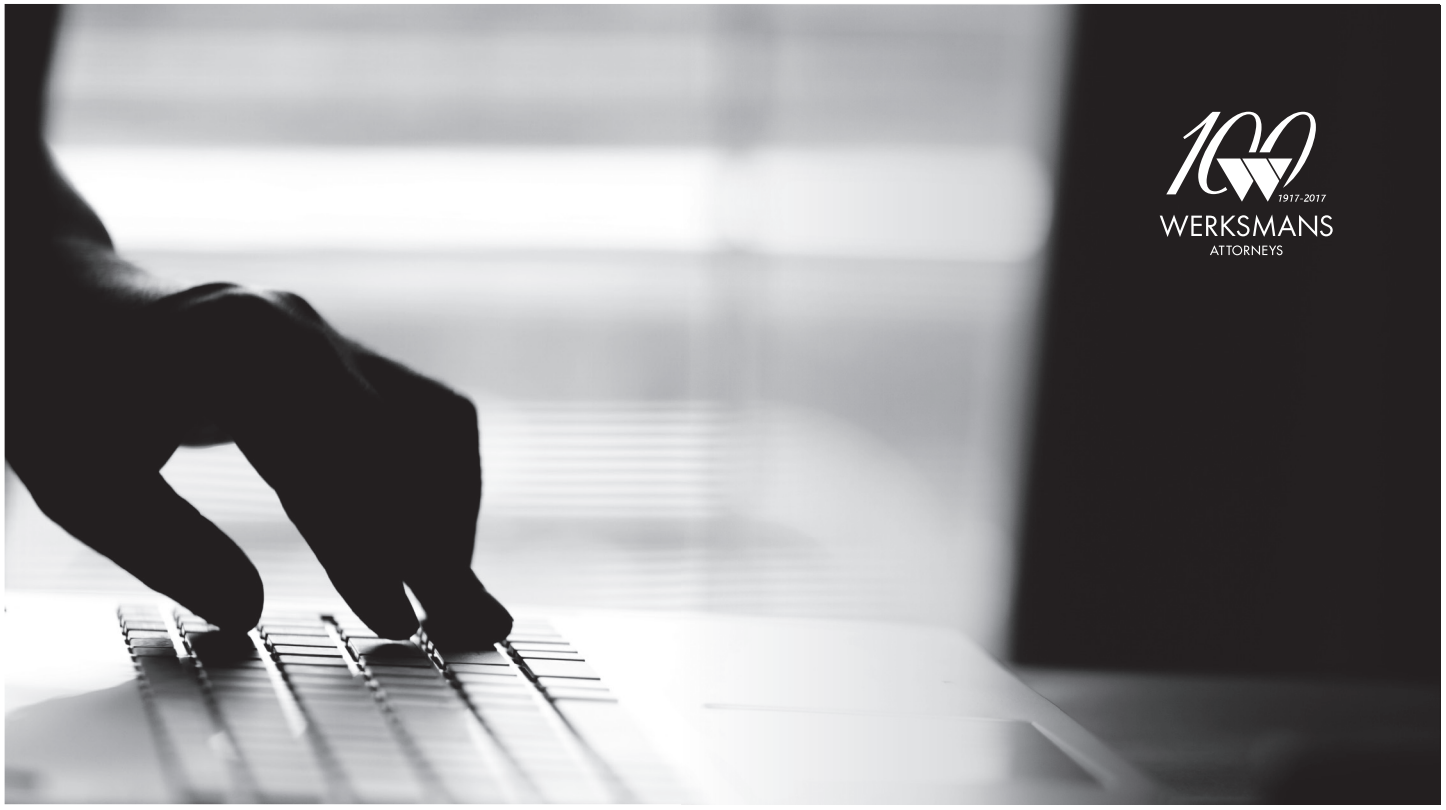

YOU HAVE TO SAY SOMETHING
AS WITH DATA DISAPPEARING, YOUR EMBARRASSMENT WILL NOT

By Director, Ahmore Burger-Smidt

LEGAL BRIEF
NOVEMBER 2017

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.

CONTACT THE AUTHOR

AHMORE BURGER-SMIDT

Title: Director, Werksmans Advisory Services (Pty) Ltd.
Office: Johannesburg
Direct line: +27 (0)11 535 8462
Fax: +27 (0)11 535 8762
Email: aburgersmidt@werksmans.com

Click here for her profile.

> Keeping you close for 100 years

The Corporate & Commercial Law Firm
www.werksmans.com
A member of the LEX Africa Alliance

ABOUT WERKSMANS ATTORNEYS

Established in the early 1900s, Werksmans Attorneys is a leading South African corporate and commercial law firm, serving multinationals, listed companies, financial institutions, entrepreneurs and government.

Operating in Gauteng and the Western Cape, the firm is connected to an extensive African legal alliance through LEX Africa.

LEX Africa was established in 1993 as the first and largest African legal alliance and offers huge potential for Werksmans' clients seeking to do business on the continent by providing a gateway to Africa.

With a formidable track record in mergers and acquisitions, banking and finance, and commercial litigation and dispute resolution, Werksmans is distinguished by the people, clients and work that it attracts and retains.

Werksmans' more than 200 lawyers are a powerful team of independent-minded individuals who share a common service ethos. The firm's success is built on a solid foundation of insightful and innovative deal structuring and legal advice, a keen ability to understand business and economic imperatives and a strong focus on achieving the best legal outcome for clients.