REGULATORY

When the law says – confess!

1 August 2018 *4 min read*

by Ahmore Burger-Smidt, Head of Data Privacy Practice

The importance of a data breach plan

The South African society has read about, and some members unfortunately experienced, significant data breaches this year already. Even the Presidency's website was targeted during July 2018. In a statement addressing the incident, Khusela Diko, who is President Cyril Ramaphosa's spokesperson said that "*we can confirm interference with the Presidency website. Our technicians are currently investigating the incident and looking to restore it to operation*".

The hackers identified themselves in the message as "Black Team X". Another case of hacktivism occurred last year in August, when an infamous cyber group by the name of Anonymous targeted gov.za sites, revoking access to the pages for a weekend.

The lesson fortunately being learned is that it's not a question of whether a company will experience a data breach, but when. The challenge is to ensure that companies are adequately prepared to successfully deal with a breach, and emerge from the experience wiser and far more robust in terms of knowledge, systems and processes. According to a recent Ponemon Institute study, data breaches are among the top three types of incidents that affect brand reputation.

The extent of stolen or leaked data is often unbelievable. Furthermore, the proactive detection of a data breach rely on advance threat intelligence capabilities and far too often a data breach is detected when it is reported in the media or the company informed by the person responsible for the breach that they have already been compromised.

Once a breach has been contained, organisations are faced with an immense clean-up operation, involving amongst others upgrading of systems, potential administrative fines and legal fees. It is undeniable that an uphill road lies ahead in terms of brand rehabilitation for those that manage to survive a data breach.

In terms of section 22 of the Protection of Personal Information Act, Act 4 of 2013 ("**POPIA**"), a company has a duty to notify the Information Regulator once a data breach took place. The notification must take place as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement and any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system. A data subject must also be notified (unless their identity cannot be established), where it has reason to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person. The POPIA states that a notification to the data subject may only be delayed if a public body responsible for the prevention, detection or investigation of offences or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned.

The good news is that there is much that can be done ahead of time to prepare for a data breach and in so doing everyone can be prepared. It cannot be stressed enough how much time this will save later in trying to determine how to respond. It is imperative to determine which messages a company will communicate from the first disclosure of a data breach through to the final investigation and steps by the Information Regulator. Companies need to consider what to say about the proactive steps they are taking based on the nature of the incident and what customers or those affected need to do and how they intend to help their customers.

In order to be prepared a data breach team is required. The size of the data breach team and its composition depend on several factors. These include the size of the company, the industry involved and the complexity of the business. At many companies the response team includes at least one representative from each of the following areas:

- Human resources
- Information technology or data security
- Communications
- Risk management
- Legal
- Senior management

It is (will be) mandatory for companies to notify the Information Regulator of a data breach once the POPIA has been fully promulgated. Companies will not be able to shy away from this obligation.

Confession is an absolute duty in terms of POPIA. One should be clear on the content of a confession. A confession could very likely bring about unintended consequences. Preparation should never be underestimated.

Ahmore Burger-Smidt

Head of Regulatory

View Profile