We've had a data breach - who do we have to tell?

By Ahmore Burger-Smidt

13 Oct 2021

Concerns over cybersecurity and data breaches are growing globally, fuelled and escalated by reports of ever-larger data breaches, the "rise of machines" and remote working. The extent and impact of a security incident largely differs depending on the sector infiltrated and the type of personal information processed within that sector.

Source: © Gleb Shabashnyi – 123RF.com

Concerns over cybersecurity and data breaches are growing globally, fuelled and escalated by reports of ever-larger data breaches, the "rise of machines" and remote working. The extent and impact of a security incident largely differs depending on the sector infiltrated and the type of personal information processed within that sector.

As a natural consequence, organisations have no choice but to manage these risks by, inter alia, implementing appropriate, reasonable technical and organisation measures to secure the integrity and confidentiality of personal information under its possession. This is recognised in terms of section 19 of the Protection of Personal Information Act 4 of 2013 (PoPIA). Furthermore, when – and not if – a security compromise occurs, organisations must understand their obligation to notify such security compromise to the Information Regulator and affected data subjects in line with section 22 of PoPIA.

However, most organisations seem to be at a loss of how to:

- effectively respond to a security compromise incident; and
- notify the Information Regulator of such security compromise.

The foregoing appears to be the case in the recent cyber attack that occurred at the Department of Justice where the Information Regulator wrote a stern letter to the Department of Justice about the "flawed way" in which it handled the cyber attack. In this cyber attack, the Department of Justice merely informed the Information Regulator that its computer systems

had been hacked and that they are still investigating the matter without indicating whether any personal information was stolen, accessed or exposed.

So, what then must organisations do?

Organisations need to understand their notification obligations to the Information Regulator, in the first instance, and affected data subjects, in the second instance, in the event of there being reasonable grounds to believe that personal information of a data subject has been accessed or acquired by an unauthorised person. The test for what are "reasonable grounds" is likely to be a hybrid objective-subjective inquiry in that:

- it is objective in the sense that the duty to notify wil only arise if a reasonable person, in the position of the organisation, would have grounds to believe that a security compromise occurred; and
- it is subjective in the sense that the duty to notify requires notification to occur "as soon as reasonably possible after the discovery of the compromise". A construction of the word "discovery" is indicative of subjective awareness of the security compromise.

  So, therefore, to the extent that the threshold of the requirement of reasonable grounds is satisfied, the Information Regulator and affected data subjects must be notified. This is an absolute, non-negotiable requirement. The only exceptions relate to when notification may be delayed which are limited to the following:

  - it is not necessary to notify affected data subjects of the security compromise where his/her identity cannot be established, but the Information Regulator must still be notified;
  - an organisation may delay notification to both the Information Regulator and affected data subjects where it is reasonably necessary for the organisation to investigate the compromise and to restore the integrity of its information systems;
  - an organisation may delay notification to the data subject if a public body responsible for the prevention or investigation of crimes or the Information Regulator determines that the notification will impede criminal investigations of the public body concerned.

  This notification obligation as set out in PoPIA differs from that of the General Data Protection Regulation 2016/679 which posits that only if the security compromise poses a high risk to those individuals affected then they should also be informed, unless there are effective technical and organisational measures that have been put in place, or other measures that ensure that the risk is no longer likely to materialise.

  Taking guidance from the remarks made by the Information Regulator regarding the poor handling of the security compromise by the Department of Justice, it is important for organisations to take cognisance of how such notification must be made to affected data subjects. To this end, PoPIA is instructive and provides that a notification to data subjects must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:

- a description of the possible consequences of the security compromise;
- a description of the measures that the organisation intends to take or has taken to address the security compromise;
- a recommendation of measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
- if known, the identity of the unauthorised person who may have accessed or acquired the personal information.

Furthermore, PoPIA prescribes that notifications must be in writing and may be by way of either:

- physical mail to the data subject's last known physical or postal address;
- email to the data subject's email address;
- placing a notice in a prominent position on the website of the organisation;
- publishing a notice in the news media; or
- as may be directed by the Information Regulator.

According to a data breach report published by IBM and the Ponemon Institute, the cost of a data breach in 2021 is $4.24 million (which is about R63 million) and this is an approximate 10% increase from the average cost in 2019 which was about $3.86 million (which is about R57 million). This cost, will no doubt, continue to soar going forward.

Considering the above, organisations should take steps, plan, prepare and safeguard themselves from potential security compromises and cyber attacks, especially given the notion of not "if", but "when" a security compromise may occur. In this way, organisations will be able to manage such risk effectively and foster customer trust and confidence which are foundational pillars of success for any organisation.

ABOUT THE AUTHOR

Ahmore Burger-Smidt, Director and Head of Data Privacy and Cybercrime Practice and member of the Competition Law Practice at Werksmans Attorneys