CYBER ATTACKS AND REPORTING OBLIGATIONS UNDER POPIA

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Tshepiso Hadebe | November 23, 2021

The month of October, known as the Cybersecurity Awareness Month, comes at a time when South Africa is reeling from the effects of a plethora of security breaches and cyber attacks that have plagued the country since the beginning of 2021. The most recent security breaches and cyber attacks targeted Transnet and the Department of Justice and Constitutional Development. Section 22 of POPIA is relevant in this regard as it provides that responsible parties have to report cyber attacks under POPIA.

On 22 July 2021, Transnet suffered a major cyber attack that saw the disruption of the company's IT systems. The state-owned company was forced to switch to manual operations, causing the company's operations to grind to a near-standstill. The attack disrupted normal processes and damaged equipment and information.

On 9 September 2021, the Department of Justice and Constitutional Development ("**DoJ**") announced that their information technology systems were interrupted due to a security breach which was effected through ransomware. This resulted in all information systems being encrypted and unavailable to both internal employees as well as members of the public. The attack affected all electronic services provided by the DoJ including the issuing of letters of authority, bail services, email, and the DoJ's website.

The Information Regulator ("**IR**") was also impacted by the security breach. In a statement issued by

the IR, the DoJ ransomware attack also impacted the work of the IR because the IR relies on the DoJ's information technology systems for its operations. This resulted in the IR's website being temporarily unavailable for three days. In the statement, the IR also expressed concern regarding the high number of security breaches in South Africa, stating that in August 2021 alone, thirty-eight responsible parties suffered and reported security breaches.

In the same breath, the IR stated that it has written to the DoJ to remind them of their obligations in terms of Section 22 of the Protection of Personal Information Act ("**POPIA**"). Section 22 requires that where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Regulator and the data subject unless the identity of such data subject cannot be established.

On 4 October 2021, the DoJ published a notification addressed to all data subjects regarding the potential compromise of the personal information of data subjects in accordance with the POPIA. The DoJ indicated that upon its analysis of the nature and extent of the breach it found that there might be personal information that had been acquired by an unauthorised person/institution whose identity is currently unknown. Furthermore, the DoJ stated that the extent of the data that has been compromised has not yet been fully determined. It has been established that at least 1200 files have been exfiltrated. These files might have contained personal information such as names, contacts and banking details. The DoJ further stated that possible consequences of the breach include the selling of the personal information and its use for unlawful purposes. It concludes by setting out recommendations that data subjects can adopt to mitigate the possible adverse effects of the security compromise. The IR issued a similar notification regarding the DoJ security breach.

The plague of cyber attacks on South African government entities has exposed the vulnerability of the government's information technology systems. It has also indicated that there is a grave need to bring the discussions on cybersecurity to the forefront. This is the right time for the Cybercrimes Act 19 of 2020 to come into full effect. The Cybercrimes Act criminalises offences such as ransomware attacks.