Short Notes on:

THE ROLE OF DIRECTORS IN THE AGE OF CYBERCRIME

Introduction

The exponential development of technology in recent years has meant that cybercrimes are no longer just an occurrence in Hollywood movies. South Africans have been the victims of numerous cyber-breaches exposing their personal information as was the case with the data leak of real estate company Jigsaw Holdings in 2017. Known to be the largest data leak in the history of the country, the incident occurred when 60 million South Africans' ID numbers, phone numbers and estimated incomes were uploaded by mistake onto the company's unsecured and publicly accessible server.[1] Although this seems shocking, internationally, the risk is just as realistic. In 2018, the Indian government's ID database called "Aadhaar" (meaning foundation) saw the records of all 1.1 billion registered citizens compromised after being a victim of breaches.[2]

The right to privacy in South Africa is protected under Section 14 of the Constitution with particular mention of the right to not have the privacy of one's communications infringed. Cyber-breaches mainly compromise this invaluable right through either unlawfully retaining, recording or sharing one's personal information.

Legislation

The Protection of Personal Information Act(PoPIA)[3] was designed to help protect this right through allowing for the establishment of an Information Regulator and also minimum requirements to be satisfied when processing personal information. Under the Act, Condition 7 stipulates that a responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable measures to prevent loss, damage or unlawful access to such personal information.

In the case of directors, the link can easily be made between a 'responsible party' as stipulated above and a director who acts as an extension of such a 'responsible party'. In this regard, included

[1] https://www.timeslive.co.za/news/south-africa/2017-10-22-data-leak-legal-delays-create-a-free-for-all/ (accessed on 24 October 2019)
[2] https://www.fin24.com/Finweek/Business-and-economy/sa-business-underplaying-the-danger-of-cybercrime-20190313 (accessed on 24 October 2019)
[3] Act 4 of 2013.

in the normal scope of directors' duties would be the addition of ensuring the safety of any personal or sensitive information obtained.

Section 76(3) of the Companies Act[4] states that a director, when acting in his/her capacity, must do so in good faith and with the degree of care, skill and diligence that may be reasonably expected of someone in his/her position acting with the same general knowledge, skill and experience. What this translates to, is that directors have an objective analysis of their work done based on the subjective criteria of someone acting with the same level of skill and intellect as that particular director in question. Failure to act in accordance with this fiduciary duty, a director could even be held personally liable for any damages incurred by the company as a result of his improper actions.

Additionally, in the King IV Report on Corporate Governance of South Africa, 2009, under a guideline of practices to be employed to further the implementation of good governance, Principle 12 recommends that governing bodies of companies 'exercise ongoing oversight over technology and information management' to a point that it results in an 'ethical and responsible usage of technology and information'. In this case, again the usage of the word 'director' is not explicitly included, but the report can be integrated into any business model if the assertion of good governance is to be made.

Conclusion

With a combination of these three pieces of legislation, one can easily see the duty directors have in terms of protecting personal information from cybercrimes. When data of this nature is leaked it can be used to commit various forms of fraud with serious financial implications for the victim. As a result, there are also rights to recourse included in PoPIA in order to hold companies and by extension, directors (even though not always directly), liable for reputational or general damages. In certain instances, the penalty can be a fine or a period of imprisonment not exceeding ten years. Penalties can be issued by the Information Regulator or a court of law, and the amount can be determined at the Regulator's/court's discretion depending on the facts and seriousness of the matter.

As the world of technology further develops, the means and resources used to conduct cybercrimes will undoubtedly become more accessible. With a growing number of instances of companies selling personal information, tighter legislation will be needed not only to protect consumers but to guide directors as to the scope of their obligations as well.

[4] Act 71 of 2008.