What are a director's duties when it comes to cyber risk?

By Berné Burger & Daniel Vale

4 Sep 2018

Duties which may not have been relevant to a company director 10 years ago may now have become relevant due to the development of technology and the associated risks. These are evolving on a near daily basis posing countless threats to companies, and accordingly, directors need to stay abreast of legal developments to protect themselves and their companies in their fiduciary duties.

©Cathy Yeulet 123rf.com

The outline of such duties, in broad terms, is contained in legislation, common law and in the King IV Report on Corporate Governance for South Africa.

The law

The South African law prescribes duties that directors of companies must abide when acting and/or carrying out the functions of their office. The bulk of these duties has developed over the course of South Africa's corporate and legal history and is enshrined in the common law. Despite clearly stipulating legal obligations for directors, these duties have historically been meekly enforced, giving directors wide discretion in conducting company business. However, the passing of the Companies Act, no. 71 of 2008, (the Companies Act), codified particular common law duties that limited discretionary powers of directors, enforcing legal obligations more stringently.

The common law stipulates that directors have the fiduciary duties of good faith, honesty and loyalty towards their companies. Fiduciary duties are duties derived from a relationship of trust and confidence between the respective directors and the company itself. A director must, therefore, exercise reasonable care and skill when acting and/or carrying out the functions of their office in terms of the common law.

The duty of reasonable care and skill is judged subjectively: A director is expected to only exercise the degree of care and skill expected from a director with their particular set of skills, experience and ability. Should a director be less qualified than another, they would be judged on a lower threshold and, accordingly, expected to exercise less "care and skill". In essence, a director's ignorance and/or inexperience would protect them from liability, since less would be expected from them.

The passing of the Companies Act has changed this stance. Since codification of the duty of reasonable care and skill under section 76(3)(c) of the Companies Act, a more objective obligation has been imposed on directors. In terms of section 76(3)(c), a director is expected to exercise such reasonable care, skill and diligence that a person carrying out the same functions as the director, with the same general knowledge, skill and diligence as said director, would be expected to exercise. This new test is two part:

- Subjectively assessing what general knowledge, skills and diligence a director might have.
- Objectively assessing said director's conduct in light of these skills.

This codified duty in conjunction with King IV imposes obligations upon a director of a company to maintain a degree of oversight and understanding of a company's cybersecurity and risks.

King IV

King IV is the yardstick for corporate governance in South Africa and becomes compulsory if the relevant company is listed or seeks to be listed on the JSE. Outside of JSE listed companies, the principles set out in King IV are of value in providing the framework within which good governance takes place, and what companies and its directors are required to do to ensure good governance. The code provides interpretative clout when adjudicating matters of good governance too.

King IV, published in November 2016, signalled a significant change in the approach to corporate governance in light of advances in technology and digitisation that are revolutionising business and transforming products, services and business models. King IV urges organisations to strengthen the processes that help them, to anticipate change and to respond by capturing new opportunities and managing new risks.

This is perhaps best encapsulated in principle 12 of King IV, which applies to information and technology and sets out eight detailed practices that a company ought to comply with. The recommended practices emphasise the need for responsibility, continuous oversight and policies to ensure information security and management. King IV also introduced onerous disclosure requirements relevant to all its principles, including principle 12.

While the principles and recommended practices do not directly speak to a director's liability, it can have the effect of increasing the expectation of a director's duties, and an increase in duties can lead to an increase in potential liability.

If a director of a company fails to follow the recommended practices set out in principle 12, and the company suffers a cyber-attack that could have easily been avoided had the principles been followed, a court would be inclined to look at the recommended practices and the director's compliance , or lack thereof, to determine whether the director acted with the reasonable care, skill and diligence required in the Companies Act. Thus, King IV provides interpretive clout when determining the legal obligations of directors, especially so in the sphere of cybersecurity.

The legal reality

It is clear that directors of companies have acquired legal obligations to ensure the continuous oversight of policies and

happenings designed to maintain information and technology security and management at their respective companies. This duty is encapsulated in the conjoined reading of the Companies Act and King IV.

Although stipulating varying thresholds for directors with different skillsets, it is plain that all directors must maintain a degree of oversight over their companies' information and technology security. With the increased prominence of e-commerce and the digitalisation of businesses, complete ignorance in this regard can no longer be pleaded.

Moreover, when completely enforced, the Protection of Personal Information (Popi) Act will only bolster such requirements further, as directors of companies - specifically, chief executive officers - are automatically appointed as "Information Officers" and are responsible for compliance with the Act. It is pivotal that directors stay in tune with the duties with which they are obliged to fulfill in the developing world of information and technology.

ABOUT THE AUTHOR

Berné Burger is an associate and Daniel Vale, a candidate attorney at Webber Wentzel