BIZCOMMUNITY

Cybersecurity breaches: Can you afford not to be insured?

By Andrew Naidoo

8 Dec 2023

Companies have long known that their information may be open to attack from digital pirates. The digitalisation of most aspects of business and the growing sophistication of hackers' strategies, results in the average company not keeping pace in employing adequate cyber risk control measures.

Image source: Jakub Jirsak – 123RF.com

The current economic crisis creates a real threat of losing clients but to lose clients and your reputation because of the actions of external parties is much more devastating. The need for cybersecurity insurance continues to increase whether your business is small or large, in construction or finance, in the field or in an office.

General insurance policies do not include cyber risk cover, some specifically exclude it. Where included, specific requirements need to be met for indemnification of a claim and thus policy interpretation becomes paramount.

Recent breaches in network security at large corporates, and governmental departments have alerted the public to the risk of their personal information being disseminated without their consent and the potential of loss. The Protection of Personal Information Act, 4 of 2013 caters for companies and directors to be held liable for such loss.

The Information Regulator recently issued a R5m fine to the Justice Department for failing to comply with an enforcement notice. A warning to corporates of the risk of being penalised for breaches in network security. The cumulative costs of a network security breach could run into the millions of rands. No business can afford to have a claim rejected for failing to comply with the terms of their insurance policy.

The cost of no antivirus software? R5m, says SA Information Regulator

Ahmore Burger-Smidt and Nyiko Mathebula 4 Jul 2023

Requirements and interpretations

A cyber insurance contract has its own unique requirements which must be met to prevent a rejection of a claim. In interpreting an insurance contract, a court will have regard to the literal meaning of words in the contract, and if it yields a fair and reasonable result considering the purpose of the policy.

A court will not readily come to the aid of a company who complains the terms of insurance ‘drive a hard bargain’, nor will it interpret exclusions in favour of the insured because it considers them to be unfair or unreasonable.

Cybersecurity insurance offerings differ across insurers but what is common in all policies is the need for the client to consistently be employing effective risk control measures. What this entails is not easily apparent to every business owner.

Companies must therefore obtain professional advice on the terms of their current insurance policies, to ensure that they are in the best position to successfully claim against their insurers should a cybersecurity breach occur.

ABOUT THE AUTHOR

Andrew Naidoo is a Senior Associate in the Litigation Department of Garlicke & Bousfield Inc.