WERKSMANS
ATTORNEYS

DISPUTES

Cybercrimes and Business Interruption

1 February 2023 *5 min read*

by Darren Willans, Director, Sarah Passmoor, Director and Chiara Ferri, Candidate Attorney

Cybercrimes and Business Interruption are becoming increasingly prevalent in the technological age, posing a potentially significant threat to companies, especially those with online business models. If your company stores significant customer data, you may be targeted for ransomware attacks, as well as other sinister forms of cybercrimes. Cyber insurance should therefore be an essential aspect of a company's risk strategy in response to this form of business interruption.

In 2021, cyber incidents were ranked as one of the highest threats to businesses in South Africa, having increased by 150% since 2020. Because this area of insurance law is constantly evolving and can be vague, it is essential that your company ensures that the policy clauses are not only clear and unambiguous, but also that the policy is up to date so that it caters for the current cyber risks, which are evolving at a rapid pace.

South Africans must up their game against cybercrime

Many businesses are operating under the false belief that their current insurance policy adequately covers data security and privacy exposure. This is not necessarily the case, as traditional insurance policies often do not adequately cater for the exposure organisations face in this sphere. Companies are in this regard cautioned to be particularly mindful of specific aspects of their insurance coverage, some of which are set out below.

The all-risks clause

A potential issue that may arise in a business interruption claim, is where a cybercrime is only covered under all-risks clauses. All-risks policies have historically included claims for business interruption, which respond to loss arising from physical damage to property. This may prove problematic if your business is subject to a cyberattack, as "**physical damage resulting in financial loss**" typically does not cover ransomware attacks, or other cybercrimes.

This is because electronic data or information is often not interpreted as having a physical existence. As such (in the absence of special extensions under the policy), a cyberattack and cybercrimes affecting electronic data, and in turn causing an interruption to one's business, is often not covered under an all-risks clause, as physical damage to property is not something that is easily established.

Time deductibles and indemnity periods

Another aspect of general liability clauses which may prove problematic in the face of a cyberattack is that all-risks clauses often include time deductibles and indemnity periods, stating that loss coverage only begins after a specified period. However, a cyber-attack lasting for a fraction of the applicable time period could be devastating for a business.

For example, in 2016 Delta Airlines experienced a network failure for 6 hours, which cost the airline approximately USD 150 million. Another example is the Facebook outage of 2021, also only lasting for approximately 6 hours, which resulted in a decrease in revenue of over USD 60 million.

The nature and quantum of the loss

Establishing a cause and identifying the nature and quantum of the loss incurred is a further aspect to be mindful of insofar as your insurance contract is concerned. Damage to property is generally easier to prove than establishing a virtual cause. This is all the more reason for your company to ensure that an estimated quantum and the potential nature and cause of a cyberattack, is clearly delineated in the relevant policy.

Coverage for ransomware

Whilst most stand-alone cyber policies cover ransomware as a peril, not all policies offer the necessary coverage for losses associated with it. Coverage for loss associated with ransomware should fall under "cyber-extortion coverage". This coverage should ensure that extortion payments are accounted for, as well as coverage for an IT forensic investigator who would be required to asses what data has been accessed, as well as the level of sensitivity of that data.

Third-party coverage

Companies may also be **held accountable for third-party liability** in relation to privacy and security incidents and should therefore have coverage which protects the company (as the insured) for liability resulting from the loss of personal and corporate confidential information. The coverage should extend to the failure to protect client records and data, intellectual property infringement through mismanaging customer data, impaired customer access to the insured's computer systems and privacy intrusion through cyber activity.

It is important to bear in mind that a company itself does not necessarily have to be the target of a cyber-attack, to be affected. Cybercrimes can permeate a company's suppliers and outsourced technology providers, which may in turn cause collateral damage to the company.

The insurance industry as a whole seems to be moving toward tackling cyber business interruption risks by consulting with IT security companies, not only to calculate risk but also to provide for specific delineated coverage in this area. Very few cases have to date been tested in court. From a risk mitigation perspective, companies are advised to carefully analyse the scope of their cover and to have careful regard to the wording of their policies.

Not every crime is a cybercrime – The dichotomy of cyber-enabled crimes and cybercrimes

Darren Willans

Director

View Profile

Sarah Passmoor

Director

View Profile