COVID-19: An update since our last note

Managing a business remains challenging and the insurance industry is in the spotlight. This note avoids current industry debate but rather covers three areas of concern that clients and especially business owners should consider carefully: liability, cyber and Sasria. We encourage clients to contact their advisers to determine detailed needs and discuss specific policy wording.

Effect of COVID-19 on short-term insurance

These are extremely challenging times for individuals, families and businesses. COVID-19 has required many corporate policyholders to implement expanded remote work strategies that could become normal for certain business sectors in future. These strategies can increase risks including the risk of cyber-attacks. While we have covered the subject via numerous editions of the *InShort* client communication, recent examples covered in the media encourage a reminder. Policyholders are advised to review their cyber insurance programmes, to assess the adequacy of cover for the emerging threats created by the new digital work environment and to minimise the risk that cover is not adequate. Given the prevailing economic climate, we also encourage discussion with your adviser on Sasria cover.

Shareholders and other stakeholders could challenge a business should they fail to respond appropriately to COVID-19 concerns

COVID-19 raises several liability concerns particularly if guests, customers or employees allege that they became sick due to a business's negligence. General liability insurance protects your business from financial loss, should you be liable for property damage or personal injury caused by your services, business operations or employees. It can protect you from costs associated with bodily injuries, damage to third-party property, personal injuries, medical expenses, litigation and more. When it comes to COVID-19, general liability policies should provide cover and allow you to defend claims (this is however under constant review). It should be noted that in order for a claim to be valid, the claimant would also have to show the virus was contracted due to the policyholder's negligence and detail how, when and where they got sick—all of which could be difficult.

Stakeholders may contend that management failed to develop adequate contingency plans or detail how COVID-19 could impact the company's financial performance. Most Directors and officers (D&O) policies exclude cover for bodily injuries but may offer some protection depending on the specific allegations. It is thus important for businesses to review the scope of their D&O policies to confirm they are covered in the event of an incident.

Employers' liability and COVID-19

In instances where an employee believes they contracted COVID-19 at work, a few employers' liability considerations come into play. Generally, in terms of COVID-19, claims are evaluated on a case-by-case basis and cover will likely only be triggered if both of the following are true:

- The illness in question arises out of the course and scope of employment.
- The illness in question arises out of, or is caused by, conditions particular to their work and not an 'ordinary disease of life' (e.g. the common cold) to which the general public is exposed.

For any claims, it is important to remember that every situation is unique. In each scenario, you'll need to evaluate what jobs or tasks an employee was performing when they were exposed to COVID-19. Claims will be assessed individually, and a number of outside factors could determine whether employers' liability cover will come into effect. Employers should make sure they are following all regulatory protocols to properly protect their employees from contracting COVID-19 and speak with an insurance adviser to learn more about how their cover may or may not respond to COVID-19 claims.

Cyber-attacks have increased as malicious actors have exploited network vulnerabilities resulting from remote work environments

Many cyber insurance policies may fail to provide complete protection from the risk of data breaches, network shutdowns, and civil and regulatory actions created by these new network vulnerabilities. Expanded remote work arrangements will remain with us for the foreseeable future. Corporate policyholders should review their cyber insurance programmes and make modifications as necessary to cover the associated risks and potential gaps. Good cyber practices for individuals are well documented and we remind all to remain alert.

Cyber insurance has been in existence for more than 20 years, first in connection with other lines of cover, then as standalone cyber policies

The market remains a challenging one for policyholders. There is very little case law interpreting cyber policies. Despite the variation between policy forms, most cyber policies could contain the following cover:

- *Data Breach Expense,* covering standard breach response costs to retain attorneys and forensic investigators and to notify customers whose personal information has been compromised.
- *Privacy/Network Security Liability,* covering the defence and settlement of class actions and third-party claims.
- *Regulatory Claims,* covering legal fees to respond to government investigations
- *Network Interruption,* covering lost profits and extra expenses resulting from a network shutdown.

Cyber insurers also offer a range of optional cover to address specific risks, such as ransomware attacks, data restoration, and payment card liability. The scope of cover varies significantly between policy forms, and differences in policy wording may determine which losses are covered.

Potential implications of Covid on cyber

Due to risks surrounding remote work environments, some cyber policies may have gaps or imprecise wording that insurers can exploit to argue against a claim. For example:

- There has been a sharp increase reported in two types of cyberattacks during the COVID-19 crisis: (i) ransomware attacks, where hackers use malware to encrypt a company's data, then demand a cryptocurrency payment to provide decryption keys; and (ii) fraudulent transfer schemes, where hackers send forged emails to targeted employees to induce them to transfer funds to offshore accounts. These events may not fall within the standard insuring agreements and often must be added by endorsement, and the specific wording of the endorsement could determine whether cover is available.
- Many cyber policies exclude negligent network security practices—which, of course, is contrary to the very purpose of cyber insurance. We have seen exclusions for delayed software patches, use of unencrypted portable devices, and design errors affecting network traffic capacity. Such exclusions can be highly problematic, particularly during COVID-19 when network IT resources are potentially strained.

Sasria is a Short-Term Insurance Company that provides coverage for damage to property

The damage could have been caused by special risks such as politically motivated malicious acts, riots, strikes, terrorism and public disturbances. Sasria is wholly owned by the State and reports directly to the National Treasury. The cover is bought through insurance companies who have authority from Sasria to offer it. It is only available to individuals and businesses that have property in South Africa or South African waters, and the policy does not follow the territorial limits of the underlying policy. The policyholder has an option not to purchase Sasria cover, provided that they understand what they are exposed to without Sasria cover. You can speak to your adviser to arrange cover for your assets.

Sasria does not cover pandemics or any financial loss as a result of a pandemic

The cover remains unchanged even during this period of lockdown. Clients who have Sasria cover on their policies will still enjoy the normal Sasria cover for perils defined in the policy wording. The Sasria Act (the Act) limits Sasria cover to specific special risks and they are not licenced to cover infectious disease. To cover the diseases will require changing the Act. It is also subject to finding adequate reinsurance to cover this risk and the reinsurance market is currently averse to offering this cover.

Looting is excluded from the standard cover

If a riot breaks out and goods or stock are looted during the riot, Saria will not pay out as looting is not a stand-alone Sasria peril. Looting will only be covered if it occurs during an event Sasria considers relevant and for which Sasria accepts liability. Sasria does not cover personal injuries or loss of life. Lockdown has meant that liquor businesses have been burgled and alcohol stolen from premises. Sasria does not cover loss or damage due to burglaries or theft; this should be referred to the underlying insurance company for cover. If you have any other information that suggests the incident may be Sasria-related, you must liaise with the insurance company, and they will follow the normal claims process. Sasria will treat such claims like any other Sasria claims by looking at the circumstances and merits to decide whether the claim is valid.

Loss of income

The general rule dictates that the Sasria Business Interruption (BI) cover must always follow the material damage of the property listed in the policy schedule of the underlying insurer. Sasria's view is that damage in the case of COVID-19 or lockdown cannot be a claim in terms of Sasria. Should the insured suffer damage or loss that they suspect could be Sasria related, a claim should be submitted through the right channels, even if they are not sure Sasria would cover it. This will give Sasria an opportunity to investigate fully and be able to make a proper decision based on liability.

Researcher/Contributor: Marieta Wessels, Technical Short Term Specialist, PSG Insure in consultation with Sasria and SHA