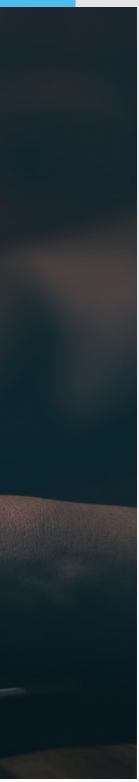
CYBER INSURANCE COVER

Santam

Cybercrime is on the rise – is your business adequately protected?

"For it is no longer a question of if, but rather "when" and "how often". I am convinced that there are only two types of companies: **those that have been hacked and those that will be.**"

– Robert Mueller Former FBI Director, March 2012



We are living in an era of unprecedented change. The risks to our world are increasing and systemic in nature. Today we face risks that did not exist a decade ago, including the challenges brought about by COVID-19 and the subsequent rapid adoption of technology. The shift to remote work has accelerated the adoption of platforms and devices that allow more transfers of sensitive data with third parties. These same capabilities have exposed users to elevated forms of digital and cyber risk. According to **Accenture**, South Africa has the third-highest number of cybercrime victims worldwide and loses around R2,2 billion to cyberattacks every year.

The Santam Insurance Barometer 2020/21 survey findings showed that **45% of commercial** intermediaries ranked cybercrime as the third-highest business risk, **while 36% of corporate and commercial entities** ranked it their **fourth-biggest risk** over the next two years. The reluctance to invest in the cyber cover seems contradictory to the survey's findings. There is still a widespread perception that "It won't happen to me" among South African businesses, as evidenced by the sizable risk protection gap in this category, which is concerning.

Cybercrime in a digital age

It is virtually impossible for any business, whether big or small, to function without connecting to the World Wide Web. While connectivity affords tremendous opportunities for businesses to use technology in a way that can improve efficiency, quality and productivity, it also creates a hotbed of opportunities for cybercriminals.

Santam recognises the far-reaching consequences this ever-expanding cyber risk could have on a small-business owner and has tailored comprehensive cyber, privacy and media insurance solutions for small to medium-sized enterprises.

The value of insurance

At Santam we help businesses reduce and manage their risk, and if disaster strikes, we get them up and running again as quickly as possible. We continually innovate to ensure our products remain relevant to our clients' needs. We are proud to launch our new cyber insurance offering available to all our existing and new Commercial clients effective 3 May 2022.

Who can benefit from our cyber insurance offering?

The offering is designed to assist owners of small to medium-sized businesses, who may suffer the loss, compromise, or theft of electronic data that can negatively impact their business, not to mention the reputational damage. Business owners can protect their business operations by means of comprehensive business insurance against the risks of digital cyberattacks.

The Santam bespoke cyber insurance offering caters for:

- Small to medium-sized enterprises
- Annual turnover of up to R20 million
- Up to 100 employees

Santam's cyber insurance offering provides the undermentioned covers up to the stated benefit limits reflected in the client's policy, for insured cyber events.

Our cyber insurance provides cover for:

1. First-party Expenses
Once a breach occurs, there are costs and expenses to get the business back on track. This extension covers the following costs: to restore data; costs of specialists, investigators, forensic auditors or loss adjusters. We will pay on your behalf any reasonable and necessary costs to restore your data and software after a data breach, to the closest possible condition in which they were immediately before the data breach.

2. Business interruption
We will pay you for your reduction of net profit during the interrupted period which has been directly caused by a cyber incident.

3. Reputational Management Expenses
Every business cares about how its customers perceive it. This extension covers the costs of a public relations consultant or related advertising expenses to mitigate any reputational or material brand damage.

4. Administrative fines and penalties imposed by any supervisory authority to extent insurable by law.
Legislation such as POPI (Protection of Personal Information) introduced the imposition of hefty fines, penalties and even jail time. This extension covers the legal defence costs against the sanction as well as the amount of the actual fine or penalty itself (as long as the regulator allows it to be insurable).

5. Media Liability
Most organisations use websites, social media platforms and other electronic media, and there is always a risk of copyright or defamation allegations. This extension covers the legal defence costs, legal liability to pay damages, public relations communication costs, and claims expenses arising from the performance of online media activities.

6. Theft of Funds
Businesses that have suffered a network security breach may find that funds have been taken by unauthorised third parties. This extension covers you for any money illegally taken from you as a direct result of cybercrime.

7. Notification Expenses
There will be costs to notify affected parties and monitor any possible identity theft. The policy covers the expenses incurred to comply with privacy legislation and includes legal and communication expenses as well as credit monitoring and identity theft monitoring service.

8. Cyber extortion and cybercrime
Should a business's data or system be locked or a business be threatened by cyber extortionists, there may be costs in negotiating with the hackers. This extension covers costs of the investigation into the cause of, or the payment of monies (where legally permissible and subject to our prior written consent) in response to or as a result of an extortion threat.

The importance of risk management

Cybercrime is a complex and continuously evolving risk that requires more attention than it is currently receiving. The human element has always been the biggest risk within any business's computer system or cyber security controls. Phishing attacks are specifically designed to take advantage of human nature and employee mistakes. Furthermore, suspicious emails with download instructions and phone calls aimed at getting security information from employees are still very effective gateways for cybercriminals to gain access to companies. Over and above a cyber insurance policy, awareness is key to ensuring employees are sufficiently skilled to identify potential cyberthreats and clearly understand what to do in any situation where they suspect they may be targeted by a phishing attack.

Below are some of the risk management tips companies can implement to mitigate and prevent cyberattacks.

- Increase staff awareness

- Manage staff behaviour
- Implement strong password management policies
- Consult a security specialist
- Reduce unnecessary transfer of information
- Avoid complacency with regard to data management

The role of the intermediary

We believe intermediaries are key in driving broader and sustained awareness of cybercrime. They have an important role to play in educating clients about the benefits of cyber insurance and explaining how the cover works. Such knowledge and expertise will undoubtedly be required in the case of a complex, emerging and as-yet relatively unfamiliar risk like cybercrime.

Contact details

For more information on cyber insurance, please visit
www.santam.co.za