HAMTERN • CONNECT

Insurance perspectives and updates

Data Breaches and Cyber-Attacks

By Rob Scott | Partner | Clyde & Co

Data security and cyber breaches are becoming an almost daily occurrence, as is widely reflected in increased publicity and media reports, which also demonstrate that data breaches are growing both in frequency and scope each year.

South Africa has been slow to regulate cybercrimes and data breaches. There are currently two key pieces of proposed legislation that are relevant:

- The Protection of Personal Information Act 4 of 2013 ("POPI") is South Africa's proposed data protection law aimed at addressing data privacy and security. This Act was first tabled in Parliament in 2009 and is yet to come into force.

- The Cybercrimes and Cybersecurity Bill. A second draft of the bill was introduced into parliament in February 2017. The Bill aims to consolidate offences relating to cybercrimes, as well as to create new cybercrimes and offences in order to bring South Africa in line with relevant international conventions and model laws.

Notwithstanding that this proposed legislation is not yet in force, it is critical for organisations to consider the impact that data breaches or cybercrimes might have on their businesses. Data breaches may erode the confidence of customers or clients, may have a major impact on an organisation's day to day business activities, may significantly impact sales and/or reputations of organisations and render organisations legally liable to third parties. To be more specific:

- Data breaches and/or cyber-attacks often require that networks be taken off-line to prevent further data loss, which result in business interruption losses and reputational damage.
- Organisations often need to employ the services of legal experts and/or forensic experts to investigate whether a breach has occurred and what the extent of that breach is.
- Organisations that are victims of data breaches or cyber-attacks may be contractually liable to business partners in the event of data security breaches. These contractual obligations can often include significant financial penalties and/or result in a breach or cancellation of vital contracts. Organisations may even be contractually liable to other contracting parties in respect of any data breaches
- or cyber-attacks.
  In due course, and once the relevant legislation has been promulgated in South Africa, organisations may be liable for notification costs, regulatory investigation costs and/or litigation costs, including criminal sanctions, damages and/or penalties payable for data breaches or cybercrimes.

It is critical for organisations to take steps to mitigate any risks (including reputational) and costs that flow from data breaches or cyber-attacks: this is because it is highly likely that an organisation, notwithstanding the preventative measures put in place, will suffer some form of data breach or cyber-attack in the near future.

One manner of mitigating these costs or risks is for organisations to assess whether or not they require comprehensive cyber insurance coverage to assist them in covering any costs incurred in the event of a data breach or cyber-attack. Without comprehensive cyber insurance cover, organisations may be left to pick up all these costs by themselves. Such costs can be significant and even cripple a business.

The Personal Data Protection Commission in Singapore recently issued various guidelines for organisations to adhere to in order to protect personal data, these being:

- An inventory should be taken of the type of data an organisation handles.
- Data should be categorised according to its sensitivity, and policies should be implemented appropriate to each classified type of data, especially in instances of sensitive data.
- Risk assessments of an organisation's systems, processes and practices should be conducted.
- Technological measures should be implemented to protect data.
- Employees should be made aware of their obligations to protect personal data.
- There should be limited access to personal data, and secure passwords should be implemented.
- Encryption of data should be utilised.
- Audit logs or other physical measures should be put in place to trace unauthorised access, and own systems should be audited periodically, as well as those of vendors, in order to test vulnerabilities.

In addition to this, it is necessary for organisations to question what security protocols or programmes are in place to deal with data breaches or cyber-attacks, as well as to develop and implement comprehensive incident response plans, to ensure that their response is both quick and effective.

In light of the more frequent and increasingly sophisticated cyber-attacks and incidents occurring almost daily across the globe, including South Africa, organisations will do well to expand their efforts to mitigate the consequences of inevitable data breaches. The primary objective for organisations at this juncture should be to implement measures that will serve to mitigate the extent of and to manage any potential cyber-security event or data breach so as to limit liability, increase client/customer confidence, ensure reduced recovery time and costs, and to keep any reputational damage to a minimum.

Reproduced by kind permission of Camargue Underwriting Managers

CONTACT US

Tel: 011 844 3900
Fax: 011 234 9562
Email: insurance@hamtern.co.za
www.hamtern.co.za