Publication: Business Day (Late Final), Business Law & Tax
Date: Thursday, February 01, 2018
Page: 10

How safe from cyber attacks?

Sharmila Naidoo
Shepstone & Wylie

Cybercrime is an increasing global threat which has caused substantial damage over the years to public and private companies such as Maersk, Google, Yahoo, Rosneft, FedEx and Telkom.

Cybercrimes can take the form of data loss, data breaches and data ransom. SA reportedly has the third highest number of cybercrime victims worldwide, losing about R2.2bn a year to cyber attacks and suffering more cyber attacks than any other African country.

These cyber attacks cause major disruptions and have serious financial implications for companies as well as for their clients.

It is estimated that the global cost of cybercrime will reach $2-trillion by 2019.

Interestingly, a leading study showed 48% of data security breaches are caused by acts of malicious intent, and that human error or system failure account for the rest. For commercial reasons, many losses and data breaches are not reported.

LEGISLATION

SA has introduced legislation such as the Cybercrimes and Cybersecurity Bill and the Protection of Personal Information Act 4 of 2013 to minimise these threats. Some of the prominent features of the Cybercrimes and Cybersecurity Bill include criminalising cybercrime and regulating jurisdiction.

The Protection of Personal Information Act promotes the protection of personal information by requiring public and private bodies to comply with certain standards from the time personal information is collected to the point of sharing. It also regulates the right to protection against the unlawful collection, retention, dissemination and use of personal information.

So, what can you do? Effective cyber management includes following available guidelines (such as the Protection of Personal Information Act), conducting regular risk assessments, adequate staff training, implementation of the correct IT systems (including firewalls and antivirus measures), insurance cover, as well as liability management in terms of third-party contracts.

You need to consider the strength of your company's own defence systems, as well as the systems of any third parties you work with and limit your contractual liability accordingly.