30 MARCH 2020

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS ALERT

COVID-19: Cyber security concerns

As a response to the outbreak and increasing number of COVID-19 cases, more companies and organisations are encouraging or instructing employees to work remotely. With an increased reliance on technology due to remote working arrangements, entities may be faced with cybersecurity challenges including cyber-attacks and cyber-related fraud. We outline some considerations for organisations below.

CDH
CLIFFE DEKKER HOFMEYR

COVID-19: Cyber security concerns

As a response to the outbreak and increasing number of COVID-19 cases, more companies and organisations are encouraging or instructing employees to work remotely. With an increased reliance on technology due to remote working arrangements, entities may be faced with cybersecurity challenges including cyber-attacks and cyber-related fraud. We outline some considerations for organisations below.

Does your company have an information security or similar policy in place?

We advise all organisations to review their information security policies and to educate employees on best practice. Of particular relevance in the present circumstances should be organisations' incident response plans and how the organisation will react in the case of a data breach or cyber-attack. Policies should outline practical steps which employees can take in the event of an alleged or actual data breach or cyber attack, including who to contact and the contact details of that person(s), the procedure for escalation and how to minimise losses.

We recommend that organisations circulate their incident response plans and information security policies to employees and draw attention to the relevant provisions to ensure employees are familiar with the steps to follow. To the extent that an organisation does not have a policy or response plan in place, we recommend drafting basic guidelines which are specific to the current challenges posed by COVID-19 and which addresses the most pressing and important risks which may arise, and circulating this as soon as possible.

Organisations should actively monitor the relevant regulatory authorities for updates or changes regarding COVID-19 and ensure that their policies and plans are updated to align with the latest official rules or recommendations from credible institutions such as the Centre for Disease Control and Prevention, the relevant government authority or the World Health Organisation. This may include updates to the number of days an employee should self-quarantine if they have potentially been exposed to COVID-19, the number of persons that may congregate at the office at the same time, or the manner in which COVID-19 is transmitted.

Oh no, I was phished! What can I do?

You should immediately report any fraudulent activity to your IT department and change all of your passwords and restart your computer.

If you are worried that you or your business are at risk as a result of the phishing incident or someone has hacked into your system or is holding some of your data ransom, you should report this to the South African Police Services and ask them to open up an investigation. You should work with your company and consider hiring an IT security company or private investigator that specialises in cybercrime investigations to assist you.

Phishing, hacking, identity fraud and computer-related extortion are currently offences under sections 86 and 87 of the Electronic Communications and Transactions Act 25 of 2002. A person found guilty of these offences faces a fine or imprisonment of up to 5 years. A fraudster can also be tried for fraud and theft under the common law.

If you are able to locate the perpetrator, you can also bring a delictual claim against them and receive monetary compensation for any financial losses suffered. You can also bring an interdict against the perpetrator to prevent them from sharing any of your data and get them to return data that is in their possession to you.

COVID-19: Cyber security concerns

Can I be held liable for distributing 'fake news' about COVID-19?

The publication and dissemination of 'fake news' in South Africa is not generally prohibited but new regulations published under the Disaster Management Act, 2002 on 18 March 2020 regarding COVID-19 state that *"any person who publishes any statement, through any medium, including social media, with the intention to deceive any other person about (a) COVID-19; (b) COVID-19 infection status of any person; or (c) any measure taken by the Government to address COVID-19, commits an offence and is liable on conviction to a fine or imprisonment for a period not exceeding six months, or both such fine and imprisonment."*

The intention of the regulation is to avoid the malicious spreading of false news and unnecessarily creating panic in the public. The public should critically review information it receives about COVID-19 and the source of such information. The above quoted regulation is limited to the publishing of any statement regarding COVID-19 and not generally to 'fake news' (in the colloquial understood sense).

When sharing information regarding COVID-19 on social media, it is imperative to ensure that this information is obtained from accredited institutions such as official government channels of communication, medical journals, the World Health Organisation or the Center for Disease Control and Prevention.

To quote the director-general of the World Health Organisation, Tedros Adhanom Ghebreyesus, "*We're not just fighting an epidemic; we're fighting an infodemic. Fake news spreads faster and more easily than this virus, and it [is] just as dangerous*".

CDH is a Level 1 BEE contributor – our clients will benefit by virtue of the recognition of 135% of their legal services spend with our firm for purposes of their own BEE scorecards.

CDH
CLIFFE DEKKER HOFMEYR

OUR TEAM

For more information about our Technology, Media & Telecommunications practice and services, please contact:

Christoff Pienaar
National Practice Head
Director
T +27 (0)21 481 6350
E christoff.pienaar@cdhlegal.com

Fatima Ameer-Mia
Director
T +27 (0)11 562 1837
E fatima.ameermia@cdhlegal.com

Preeta Bhagattjee
Director
T +27 (0)11 562 1038
E preeta.bhagattjee@cdhlegal.com

Simone Dickson
Director
T +27 (0)11 562 1249
E simone.dickson@cdhlegal.com

Aphindile Govuza
Senior Associate
T +27 (0)11 562 1090
E aphindile.govuza@cdhlegal.com

Nikita Kekana
Associate
T +27 (0)21 481 6334
E nikita.kekana@cdhlegal.com

Liam Sebanz
Associate
T +27 (0)11 562 1625
E liam.sebanz@cdhlegal.com

BBBEE STATUS: LEVEL ONE CONTRIBUTOR

Cliffe Dekker Hofmeyr is very pleased to have achieved a Level 1 BBBEE verification under the new BBBEE Codes of Good Practice. Our BBBEE verification is one of several components of our transformation strategy and we continue to seek ways of improving it in a meaningful manner.

JOHANNESBURG
1 Protea Place, Sandton, Johannesburg, 2196. Private Bag X40, Benmore, 2010, South Africa. Dx 154 Randburg and Dx 42 Johannesburg.
T +27 (0)11 562 1000 F +27 (0)11 562 1111 E jhb@cdhlegal.com

CAPE TOWN
11 Buitengracht Street, Cape Town, 8001. PO Box 695, Cape Town, 8000, South Africa. Dx 5 Cape Town.
T +27 (0)21 481 6300 F +27 (0)21 481 6388 E ctn@cdhlegal.com

STELLENBOSCH
14 Louw Street, Stellenbosch Central, Stellenbosch, 7600.
T +27 (0)21 481 6400 E cdhstellenbosch@cdhlegal.com