30 MARCH 2020

DISPUTE RESOLUTION AND TECHNOLOGY, MEDIA & TELECOMMUNICATIONS **ALERT**

IN THIS **ISSUE**

Do flexible and remote working arrangements constitute a cybersecurity threat?

The era of the millennial workforce and the rise in technology and connectivity has required a dynamic shift toward flexible and/or remote working arrangements in South African corporate spaces. These flexible working arrangements, which are designed to depart from the notion that employees need to physically attend the office during traditional working hours, usually envisage scenarios where employees can clock in their hours from the comfort of their own homes, a coffee shop or even abroad. As a response to the COVID-19 pandemic, more companies and organisations are encouraging or instructing their employees to work remotely.

CDH
CLIFFE DEKKER HOFMEYR

Do flexible and remote working arrangements constitute a cybersecurity threat?

Employees who work remotely and use public networks whilst doing so, such as the free WIFI available in cafés or airport lounges, are therefore vulnerable to the increasing threat of cyber-attacks.

The era of the millennial workforce and the rise in technology and connectivity has required a dynamic shift toward flexible and/or remote working arrangements in South African corporate spaces. These flexible working arrangements, which are designed to depart from the notion that employees need to physically attend the office during traditional working hours, usually envisage scenarios where employees can clock in their hours from the comfort of their own homes, a coffee shop or even abroad. As a response to the COVID-19 pandemic, more companies and organisations are encouraging or instructing their employees to work remotely.

With an increased reliance on technology due to remote working arrangements, companies may be faced with cybersecurity challenges including cyber-attacks and cyber-related fraud. Despite cyber security software that may be available to employees, there is an added inherent risk in accessing a company's network from any location other than the workplace. Employees who work remotely and use public networks whilst doing so, such as the free WIFI available in cafés or airport lounges, are therefore vulnerable to the increasing threat of cyber-attacks.

The most common forms of cyber-attacks include the interception of email correspondence and phishing scams. This often occurs when cybercriminals monitor the servers of either the sender or recipient of an email communication and strategically intercepts the communication by posing as a sender.

Employees should also be aware that there has been an increased number of reported phishing scams on email related to the COVID-19. There are reports of fraudsters impersonating agencies such as the World Health Organization, a company's human resources department or other government agencies enticing people to open up attachments or to click on links with information regarding COVID-19. Attackers are then able to push malware, ransomware and attempt to gain access to a personal information and passwords.

Email interception, hacking, identity fraud and computer related extortion are recognised as offences under the Electronic Communications and Transactions Act No 25 of 2002 (ECT Act), and the maximum penalty is a fine (unspecified) or imprisonment for a period not exceeding 12 months. The Cybercrimes Bill [B6 of 2017] will, once effective, create a variety of new offences which do not currently exist in South African law and afford companies with a degree of comfort relating to the prosecution of cybercrime offences.

Although South African law currently does not specifically impose a duty to implement cybersecurity measures in an organisation, the Protection of Personal Information Act No 4 of 2013 (POPI Act) (the substantive provisions of which have not yet commenced) does contain obligations on responsible parties (data controllers) to implement reasonable technical and organisational measures to safeguard personal information in their possession or control against unauthorised access, which will likely include adopting cybersecurity measures.

CDH
CLIFFE DEKKER HOFMEYR

Do flexible and remote working arrangements constitute a cybersecurity threat?*...continued*

Companies should insist that any remote working arrangement should occur via its designated digital channels for remote working, such as VPN's or servers.

According to the latest annual Cost of a Data Breach Report, conducted by the Ponemon Institute, the average cost of a data breach in South Africa is approximately R43,3 million. As a result, flexible and remote working arrangements may pose a substantial and costly risk to employers from a cyber security perspective.

Against this backdrop, it is imperative for business to review and adopt an information security policy which employees must adhere to. Employees should be encouraged not to connect to unsecure or public WIFI and utilise, where applicable, VPNs to protect their company's proprietary information. Common sense should also prevail, employees should check URL's before clicking on any links and beware of suspicious emails. With an increased use of teleservices such as Skype, Microsoft Teams, Zoom and the like, employees should ensure that meeting requests are legitimate prior to joining any meeting and refrain from taking 'shortcuts', such as sending documents to colleagues via unsecured instant messaging services, discussing confidential work matters on public chat platforms, saving documents to their desktop instead of on secure locations and using unencrypted personal devices for work matters. Any work should occur via the employer's designated channels for remote working, such as VPN's or servers.

Companies should insist that any remote working arrangement should occur via its designated digital channels for remote working, such as VPN's or servers.

OUR TEAM

For more information about our Dispute Resolution practice and services, please contact:

Tim Fletcher
National Practice Head
Director
T +27 (0)11 562 1061
E tim.fletcher@cdhlegal.com

Thabile Fuhrmann
Chairperson
Director
T +27 (0)11 562 1331
E thabile.fuhrmann@cdhlegal.com

Timothy Baker
Director
T +27 (0)21 481 6308
E timothy.baker@cdhlegal.com

Eugene Bester
Director
T +27 (0)11 562 1173
E eugene.bester@cdhlegal.com

Jackwell Feris
Director
T +27 (0)11 562 1825
E jackwell.feris@cdhlegal.com

Anja Hofmeyr
Director
T +27 (0)11 562 1129
E anja.hofmeyr@cdhlegal.com

Julian Jones
Director
T +27 (0)11 562 1189
E julian.jones@cdhlegal.com

Tobie Jordaan
Director
T +27 (0)11 562 1356
E tobie.jordaan@cdhlegal.com

Corné Lewis
Director
T +27 (0)11 562 1042
E corne.lewis@cdhlegal.com

Richard Marcus
Director
T +27 (0)21 481 6396
E richard.marcus@cdhlegal.com

Burton Meyer
Director
T +27 (0)11 562 1056
E burton.meyer@cdhlegal.com

Rishaban Moodley
Director
T +27 (0)11 562 1666
E rishaban.moodley@cdhlegal.com

Mongezi Mpahlwa
Director
T +27 (0)11 562 1476
E mongezi.mpahlwa@cdhlegal.com

Kgosi Nkaiseng
Director
T +27 (0)11 562 1864
E kgosi.nkaiseng@cdhlegal.com

Byron O'Connor
Director
T +27 (0)11 562 1140
E byron.oconnor@cdhlegal.com

Lucinde Rhoodie
Director
T +27 (0)21 405 6080
E lucinde.rhoodie@cdhlegal.com

Belinda Scriba
Director
T +27 (0)21 405 6139
E belinda.scriba@cdhlegal.com

Tim Smit
Director
T +27 (0)11 562 1085
E tim.smit@cdhlegal.com

Willie van Wyk
Director
T +27 (0)11 562 1057
E willie.vanwyk@cdhlegal.com

Joe Whittle
Director
T +27 (0)11 562 1138
E joe.whittle@cdhlegal.com

Roy Barendse
Executive Consultant
T +27 (0)21 405 6177
E roy.barendse@cdhlegal.com

Pieter Conradie
Executive Consultant
T +27 (0)11 562 1071
E pieter.conradie@cdhlegal.com

Willem Janse van Rensburg
Executive Consultant
T +27 (0)11 562 1110
E willem.jansevanrensburg@cdhlegal.com

Nick Muller
Executive Consultant
T +27 (0)21 481 6385
E nick.muller@cdhlegal.com

Jonathan Witts-Hewinson
Executive Consultant
T +27 (0)11 562 1146
E witts@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

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