Do flexible and remote working arrangements constitute a cybersecurity threat?

By Fatima Ameer-Mia Director at Cliffe Dekker Hofmeyr's Technology, Media & Telecommunications practice and Krevania Pillay

25 March 2020: 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.

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.

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 video conferencing services employees should also ensure that meeting requests are legitimate 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.

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