BIZCOMMUNITY

How will cybersecurity help your business comply with POPI Act?

With the new sections of the Protection of Personal Information Act (POPIA) being implemented, businesses need to tighten their cybersecurity as this will have an impact on their day to day operations.

The Act also aims at protecting the personal information of consumers and that of employees by ensuring that businesses conduct themselves in a responsible manner when they are collecting, sharing and storing information by holding them accountable should the information be compromised.

What you need to know about the POPI Act

25 Jun 2020

“Strong privacy requires protecting a user’s identity from unauthorised access and use, were as strong security requires binding a user’s identity to their behaviour to allow for authentication, authorisation, non-repudiation and identity management. When a person hears cybersecurity, they automatically think technology, forgetting that cybersecurity also involves people, information, systems, processes, culture, and physical surroundings. But for businesses this is a completely different story, dealing with people’s sensitive information requires a company to have proper security measures in place to protect that data,” says Brandon Naicker, a cybersecurity executive at LAWTrust.

Brandon Naicker, a cybersecurity executive at LAWTrust.

Rian Schoeman head of legal at LAWtrust, one of the top cybersecurity companies in South Africa says “these newly implemented POPI Act sections mean there will now be much closer scrutiny on companies when it comes to the protection of personal information. There is now an obligation on companies to disclose a data breach to the Information Regulators (IR) and every affected person,” says Schoeman.

He further adds that the Information Regulator will have the option to fine a violating company and have details of their data breaches made public, bringing the reputation of the organisation into disrepute. He further states that the act requires companies to implement security safeguards to protect the personal information of their clients and employees.

In order for companies to comply, organisations need to assess where personal information is being used, identify cybersecurity threats and weakness that could compromise the integrity of the data and put appropriate measures in place to mitigate any risks identified.

Because all organisations will be subject to POPIA Organisations should implement a robust cybersecurity program, that focuses on securing the infrastructure, network, endpoint, and the data through its lifecycle.

~~According to a study conducted by the South African Banking Risk Information Centre, South Africa has lost over R2.2 billion through cyberattacks in 2017.~~This puts various businesses under enormous pressure to comply with the POPIA to reduce chances of cybersecurity breaches since compliance failure will have severe penalties.

“Despite the size of your business, it is mandatory for businesses to comply with the POPIA. There are affordable ways Small and Medium Enterprises (SMEs) can position themselves to mitigate cybersecurity breaches, these can include encryption of data including emails, customer databases and contact info of external people. Acquiring a cybersecurity expert to train your employees on how to handle personal information and secure any breaches is essential,” says Schoeman.

Echoing Schoeman’s comment, Naicker says "to protect personal and sensitive information, companies should focus on strong authentication, using multifactor, biometric, and out of band controls, such as One Time Pin’s (OTP). Implementing a strong encryption policy, that uses a combination of digital certificates to provide a trusted identity for people, devices and things and the use of digital signatures to provide non-repudiation for secure transactions. Organisations should implement cryptography through the use of public key infrastructure (PKI), to ensure privacy and confidentiality," Naicker explains.

“POPIA is not without teeth and contains some heavy fines. Certain offences can attract a jail sentence of up to ten years and financial penalties can reach R10 million. But the major penalty any company can face is the publication of the breach and loss of confidence from the public,” concludes Schoeman.