BIZCOMMUNITY

Five tips to ensure your business reaps the POPI benefits faster

By Doros Hadjizenonos

11 Mar 2014

The Protection of Personal Information (POPI) Act was signed into law last year. It places strict onuses on businesses when it comes to handling personal information about their clients, staff and customers.

This includes, but is not limited to, their contact details and biometric and demographic information. The Act stipulates how companies may collect, handle, store and discard information, with heavy penalties for those who fail to comply.

A lot of cybercrime today is geared towards stealing personal information for financial gain. Users tend to recycle passwords, as it becomes difficult to remember different passwords for different accounts, such as social media, email and online shopping stores. Once criminals have access to this information, they can use it for identity theft or to commit fraud - it's easy to test a Facebook password against an Internet banking site, and the chances are that hackers will be successful.

What's more, many consumers don't install basic security measures, such as anti-virus software or back up files, especially on mobile devices. The fact that most people use their personal mobile devices for work purposes is concerning to businesses, as confidential information is at risk of leakage.

Falling in line with new legislation is a daunting task for any organisation. Yet, compliance with POPI is a good thing - and brings with it many opportunities for business.

Companies have a year's grace period to get their databases in order once the Act commences; this is extendable to three years under special circumstances. To help businesses get going, here are Check Point's top-five tips to assist in the protection of data, which will help with POPI compliance:

1. **Know where the data is**: Knowing what information you need to protect is the most important step. Once you know where this information resides, you can put a plan in place to secure it.

2. **Encrypt the data and control what data leaves the organisation**: Encryption ensures that data will not be accessible should it end up in the wrong hands. Employees are one of the weakest links in an organisation when it comes to data leakage. They may accidentally send confidential information to a friend who has the same first name as their line manager, for example. This could result in the leakage of personal information; as a result, the company could be liable to the law for any fines or imprisonment.

3. **Ensure mobile devices are secure**: As employees become more mobile, organisations need to take measures to

ensure that any information classified as personal, according to POPI, is protected - even on mobile devices, including smartphones, tablets and laptops. These days, it's easy to buy a mobile exploit, which takes advantage of code vulnerabilities to gain access to, and control over, a device and the data that resides on it, if it is not protected adequately. It is important that every business that has adopted a mobile workforce strategy has a security policy to effectively secure the data on these devices.

4. **Focus on the advantages of compliance**: Complying with POPI gives businesses a competitive advantage. Customers are more likely to do business with compliant organisations as they know their data will be safe. An even bigger advantage is that compliance opens doors to doing business with European Union organisations. Europe is strict when it comes to data protection - businesses may not deal with countries that do not have some kind of data protection act in place.

5. **Consider a new approach to security**: Software-defined protection from Check Point offers different layers of protection in a comprehensive security model, which assists businesses in meeting POPI requirements. At the enforcement layer, businesses implement policies to protect data, while the control layer involves creating the policy, and the management layer oversees the entire process and provides visibility of protected data. Data protection is about policy creation. Businesses should know what data can leave the organisation and what data must be encrypted.

Check Point has invested time and effort into creating solutions that protect organisations from the ever-changing threat landscape and has introduced advanced technologies to control data flowing into and out of organisations, whether the data is on the network or on mobile devices. Before, it was about protecting the machine; now it's about protecting the data, which could reside on the machine, on mobile devices or on the server.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet
- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...