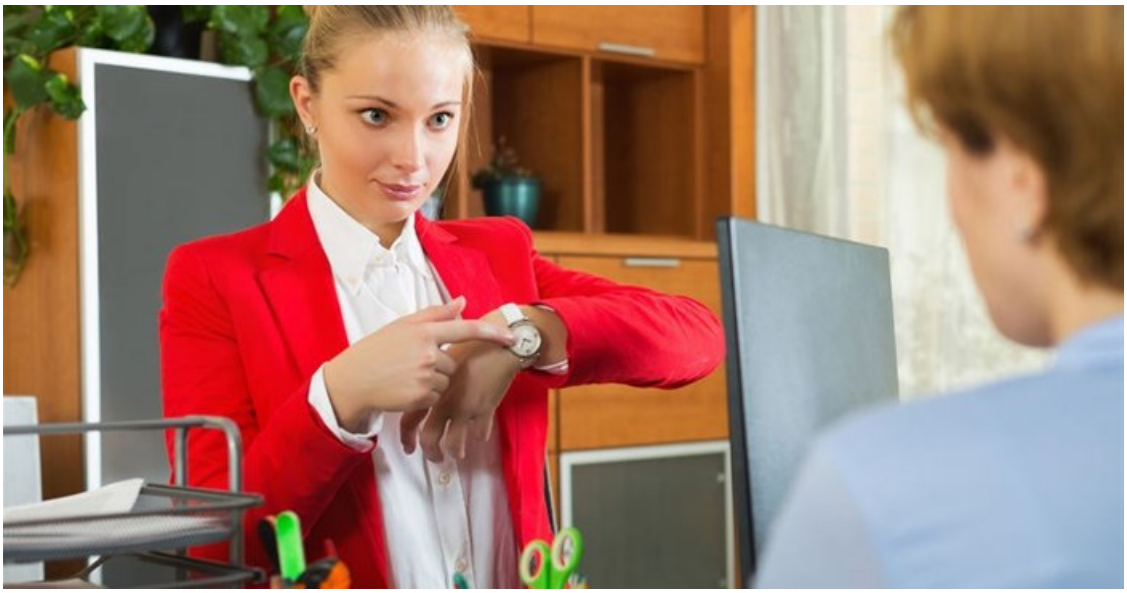
BIZCOMMUNITY

PoPI: driving organisations to make IT security a business priority

By Simeon Tassev

14 Oct 2015

Significant media attention has been given to the Protection of Personal Information (PoPI) Act over the past two years, particularly around various aspects covered and how to comply. Although the appointment of the regulator has not been finalised and there is still no fixed timeframe for implementation, it has become clear that information security needs to be made a priority.



Data breaches are on the rise, and cyber criminals are increasingly targeting the very information that PoPI is designed to safeguard. Rather than waiting for the deadline, organisations should develop a more proactive approach. Businesses that can gear themselves toward PoPI now will not only assure compliance in the future but maximise the benefits of enhanced information security in preventing data loss, leakages and breaches and their associated consequences.

Bringing information security to a business level

The growing number of high profile and well-publicised information security breaches over the past year highlights the relevance of security, and yet the majority of organisations are not doing enough to protect themselves. One of the main reasons for this is that IT security has always been viewed as an IT problem and has, therefore, never been driven by the business. This has frequently resulted in security initiatives that fail due to lack of business buy-in. This includes everything from enforcing basic level password management to high-level security initiatives and security.

In today's world, however, certain information such as customer data and confidential intellectual property is mission critical to business, and protecting it is therefore very much a business issue. This fact is clearly illustrated by the damage to businesses that breaches and data leaks can have, both in terms of reputation and recoverability. Understanding the business impact of data security is essential in driving buy-in from senior management, a critical factor for success. PoPI effectively brings information security to a business level, helping to contextualise the need for adequate data protection.

Security is a business imperative

At a basic level, PoPI seeks to regulate the processing of personal information. It aims to protect the data privacy of

consumers and will have an impact on almost every company operating in South Africa. It establishes a code of conduct for the confidential handling of personal information of visitors, customers and staff in order to ensure their privacy so that they do not become victims of crimes such as identity theft. Security lies at the heart of all of these requirements.

Customer information exists in virtually every data centre and failing to safeguard this information can damage reputation, impact operations, and result in regulatory violations, fines, and legal fees. Consequently, in order to comply with PoPI, there are a number of processes, policies and procedures that need to be put into place. However, the reality is that these all represent best practices around security, and proactive implementation can benefit businesses in a number of ways. As a result of PoPI as well as extensive media coverage of the impacts of insufficient data protection on business, security is increasingly becoming a business imperative.

Taking PoPI on board

While PoPI does not provide specific technology requirements for the protection of information, it does provide guidelines on the processes that must be put into place. This in turn will help to provide direction for the technology implementation. By taking PoPI on board, businesses are able to more effectively understand their processes by identifying and classifying their information. In addition, this helps to streamline processes, as it enables organisations to better ascertain which data is mission critical and must be protected, and which data can be safely and defensibly deleted.

From a business perspective, adequate data security is essential to prevent data breaches and compromises, which can be immensely costly. In addition, going through the implementation exercise ensures organisations effectively review processes and procedures, improve data management, optimise processes and streamline the business. Ultimately, however, despite these benefits, initiatives driven by compliance and legal enforcement are more likely to be a success due to the very clear business driver behind them. PoPI fulfils this role within the data security space, ensuring that organisations implement best practice data and information security solutions.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa
- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...