# Where to start on your journey toward PoPI compliance

By Simeon Tassev

17 Aug 2015

The much talked about Protection of Personal Information (PoPI) Act is now imminent, and organisations need to realise that the question is no longer around whether it will be implemented, but what they should do to gear up for it. Security of personal information needs to become a top of mind priority for all businesses. However, it is often difficult to know where to start, as it can be challenging to identify all of the potential sources and repositories of information covered by the Act. Email, as the primary means of communication in the modern organisation, is the ideal starting point, and will provide organisations with the first stepping-stone on the road to compliance.

With regards to PoPI compliance, organisations are typically faced with two challenges - processes and people. While technology is available that can assist organisations to comply, the processes are an essential backbone to guide the technology. In addition, an organisation can have the best processes and technologies in place, however, without educating and addressing the human component, the possibility for human error remains.

©Myimagine via Fotolia

## The nature of the technology

Email, as the main communication tool in the vast majority of organisations, plays a significant role when implementing processes and workflows. In addition, a large proportion of an organisation's Intellectual Property (IP) typically resides in email. The nature of the technology itself means that it incorporates metadata that can prove the chain of custody of information, an essential component of information regulation, and thus of PoPI. As such, it is the ideal starting point on the journey towards PoPI compliance.

The prevalent nature of email, however, does pose another challenge. Many of the processes and a lot of back-end systems in an organisation, such as workflow, Customer Relationship Management (CRM) and more, are all linked to and make use of email. It is essential to have controls in place to ensure these systems do not accidentally send confidential information to the wrong people. In addition, in a digital era, mobility is the future, and having access to email on mobile devices is an essential cornerstone of mobile productivity. However, this is a risk for business as it could potentially create data exposure over which they have no control.

## The single biggest risk

Furthermore, email is the main mechanism for a host of cyber attacks, including malware, phishing and social engineering. Email, while it is without a doubt the most used and useful communication tool, also represents the single biggest risk for organisations. It is, therefore, crucial to ensure email data security and data leak prevention solutions are put into place as part of any PoPI compliance initiative.

Developing a compliant email strategy requires that organisations firstly identify and map the process of email data flow as well as the various components. This is the first, most important and often most challenging step. From there, organisations need to demonstrate that this data is protected and controlled, that the organisations are aware of all of the data touch points and storage points and who has access to it. Technology provides the essential enabler in meeting the security requirements of these various components.

## Chain of custody is critical

Platforms should be scalable, to allow for future growth without the need to rip and replace or migrate solutions in a few

years. In addition, it is essential for email solutions to be resilient to provide continuity in case one part of the system fails. The platform also needs to incorporate security measures, and provide information to prove that a full chain of custody is maintained. Once organisations have a platform in place to provide mail services, they need to examine peripheral services around the email function, including additional security such as data leak prevention.

Bolting these features and services on to a legacy email solution often results in a disjointed and fragmented environment, so an integrated solution built from the ground up with these factors in mind is essential. With regards to PoPI compliance, chain of custody is critical. Incorporating these various technologies into an integrated platform will ensure that all of the metadata is consolidated and stored with the email, providing the required chain of custody information easily and on demand.

Given the importance of email as a communication mechanism and its prevalence in most organisations today, it is a sensible and effective starting point for PoPI compliance. Addressing email effectively, including factors such as archiving, continuity and security, will take organisations most of the way on their journey to ensuring their electronic information is PoPI compliant.

## 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...