JUTA
POPIA PORTAL

ISSUE NO 36 • ISM (INFORMATION SECURITY MANAGEMENT) TIPS FOR SMES – BYTE 9 • JULY 2024

ISM (INFORMATION SECURITY MANAGEMENT) TIPS FOR SMEs – BYTE 9

Disclaimer: We are not 'information security management' experts by any stretch of the imagination. This article includes purely practical recommendations on ISM tips which we have found helpful for smaller organisations which we have assisted with POPIA compliance issues.

Photo: iStock

1. OVERVIEW

In this byte, we look at how you should manage and respond to data breaches or incidents. Most people know about the security notification requirements in POPIA[1], but many do not know that the Cybercrimes Act[2] also places obligations on certain organisations. With recent high-profile cyberattacks like Discovery Insure and the Department of Justice and Constitutional Development, the urgency to know what to do and when is extremely important.

2. THERE'S BEEN AN INCIDENT: WHAT NOW?

Both the Cybercrimes Act and POPIA aim to enhance information security, but they have different focuses and reporting obligations. The Cybercrimes Act emphasises the criminal aspects of cyber incidents and mandates reporting to the police, while POPIA focuses on protecting personal information and requires notifications to the Information Regulator.

So how do you know if the Cybercrimes Act is applicable to your organisation in this situation?[3]

- Are you an Electronic Communications Service Provider (ECSP)[4]; or
- Are you a financial institution?

If you answered yes to one of these questions, then read the next section. If not, then jump ahead to section 4 'What does POPIA say?'

Photo: iStock

3. WHAT DOES THE CYBERCRIMES ACT SAY?

Photo: iStock

The Cybercrimes Act places legal obligations on ECSPs and financial institutions. If you are an ECSP or a financial institution and you do not report an incident or keep records, then you can be fined up to R50 000 for each incident of non-compliance![5] Key obligations under this act include:

3.1. Report the incident

ECSPs and financial institutions must report cybercrimes to the South African Police Service (SAPS) within 72 hours of becoming aware of the incident. This ensures that law enforcement agencies can take timely action to mitigate threats.

3.2. Data preservation

Entities must preserve data that could serve as evidence for at least 90 days to aid investigations.

3.3. Security measures

Organisations are required to implement measures to detect and prevent cybercrimes, such as employing advanced cybersecurity technologies and conducting regular audits.

4. WHAT DOES POPIA SAY?

Photo: stock.adobe.com

POPIA focuses on protecting personal information and the key responsibilities for security compromises are:

4.1. Report the data breaches

Organisations must inform the Information Regulator and affected data subjects as soon as reasonably possible after discovering a data breach. The Information Regulator has provided a template form and guidance on how to do this.

4.2. Security measures

Companies must implement adequate security measures to protect personal information. This includes ensuring data integrity, confidentiality, and availability through physical, administrative, and technical safeguards.

5. WHAT SHOULD YOU HAVE IN PLACE?

Photo: stock.adobe.com

5.1. Create an incident response policy and plan and create awareness

It’s inevitable that there will be some sort of security compromise, whether it’s someone sending an email to the wrong person or a full-scale ransomware attack. You need to know who to inform and what steps to take.
Make sure that all employees know what to do if the POPIA strikes the fan. Having a wonderful policy and procedure hidden in someone’s drawer won’t help you.

5.2. Create template notification letters

You don’t want to rush a very important letter to your data subjects. Create a draft that you can tweak if an incident occurs.

5.3. Detect and monitor your systems

We know the 'update now' button can be annoying, but it can also save you, so make sure you regularly update your security software. If there is an option to activate 2FA or MFA[6], do it.

Protect and encrypt your data. It's become very easy to password-protect documents in Word, so take that extra step and send the password via WhatsApp. Alternatively, work in SharePoint or Google Drive and share the link securely. Try to limit access to those who really need it if you have sensitive information.

5.4. Train your employees

This is another requirement that the Information Regulator has mentioned in enforcement notices. Train your staff so they know what to do. You can even hold drills – we have fire drills, so we should be running data security incident drills. Practise, practise, practise!

6. WHAT NEXT?

Read Chapter 5 on Information Security Management. Make sure you know what to do when a breach happens – get that plan together and practise.

Read Enforcement Notices issued by the Regulator in terms of POPIA to see the consequences of mishandling security compromises.

Photo: iStock