POPI ESSENTIALS- Data Breach Management and Crisis Communications

What is a data breach?

On 13 Feb 2020, a media announcement from a major SA Bank, outlined how it had conducted a security audit on a third party supplier who provided them with SMS and email marketing and discovered that your and my client data was exposed due to poor IT security at the supplier.

This was correctly announced as a **DATA BREACH**

A data breach occurs if it is reasonable to believe that unauthorised parties may have accessed the data.

POPIA Definition: A breach has occurred when there is *reasonable grounds to believe* that any unauthorised person has accessed or acquired personal information

So if an unauthorised party ***could have*** obtained access to PI you need to alert your impacted customers and someone (this needs to be clearly defined) needs to contact the Information Regulator. A breach is not always cyber-related, you could leave a folder of papers on a bus or have a cellphone or laptop stolen.

You are also accountable for data breaches that are caused by your suppliers.

So what must you do?

Data breaches are almost inevitable, and how you manage them makes all the difference to the level of impact the breach will have on your business and your customers. POPI compliance helps you minimise the impact on your business and your clients.

You need to plan your response to a data breach to ensure that you and your suppliers respond quickly and efficiently.

You need to be ready to get into the driver's seat when a breach occurs and

know that you are fulfilling the regulatory requirements of the POPI Act.

Workshop Overview

Workshop 1 – Understand the beast, and start taming it

We start by understanding what data breaches are and what the POPI Act expects you to do about it.

By the end of the class, you will have

- A thorough understanding of what a data breach is and the potential impact on your business
- A data breach manual to use in your business and to share with your vendors
- A guide to assessing whether cyber-insurance is needed for your business and how to compare insurance products
- A practical understanding of what cyber-forensics is and what capabilities you need in your business

Workshop 2 – Get in the driver seat, get ready to respond!

Day two is a practical workshop where you draft a data breach response plan for your business.

By the end of the class, you will have:

- A generic data breach response plan that complies with the POPI Act
- A crisis communication pack that will help you protect your brand in the event of a data breach

Course Objectives

By the end of the course, you will

1. understand what the POPI Act requirements are for managing a data breach
2. know how to plan a data breach response that integrates with your IT processes and business continuity plans
3. know how to manage a data breach in accordance with ISO/IEC 27701 (the international standard for privacy and data protection)
4. know how to manage crisis communications in a way that minimises the impact on your company's reputation
5. know how to plan for managing cyber-forensics requirements
6. be able to assess cyber-security insurance options

Why attend this course?

Data breaches are almost inevitable, and how you manage them makes all the difference to the level of impact the breach will have on your business and your customers.

You need to plan your response to a data breach to ensure that you and your suppliers respond quickly and efficiently. You need to be ready to get into the driver's seat when a breach does occur and know that you are fulfilling the regulatory requirements of the POPI Act.

You are accountable for data breaches that are caused by your suppliers, so you need to put some impact mitigations in place sooner rather than later.

The course satisfies the incident management requirements of the international standard for privacy and data protection, ISO/IEC27701.

We will also touch on the key requirements coming out of the new Cyber-Security Bill.

Who Should attend ?

Business owners, managing directors, management teams of medium sized business or small businesses that handle large volumes of personal information.

The course is also useful for IT managers, operations managers, and risk or compliance officers, or any role that is included in Business Continuity incidents.

Prerequisites

Foundational knowledge about the POPI Act will be beneficial but not mandatory. No IT skills are required. Some awareness of business continuity or IT disaster recovery would be beneficial.

The course is conducted via a **Zoom meeting**.

You will need the following:

- Access to a computer with microphone and video capability that can access a Zoom meeting. You cannot conduct this course via a mobile phone.
- We recommend you have headphones or a good external speaker
- Spreadsheets will be provided in Microsoft Office Excel. You will need a spreadsheet app that can support that format.
- Access to information about your organisation such your suppliers, customers, business processes and systems, contracts, etc.

Duration

The course consists of a total of 4-hours of classroom training split into two x 2-hour modules run over 2 days.

Time commitment from you includes an additional 4 hours (approximately) to complete a practical assignment between classes. The assignment forms a practical and integral part of your real-world POPI compliance programme.

Course Cost

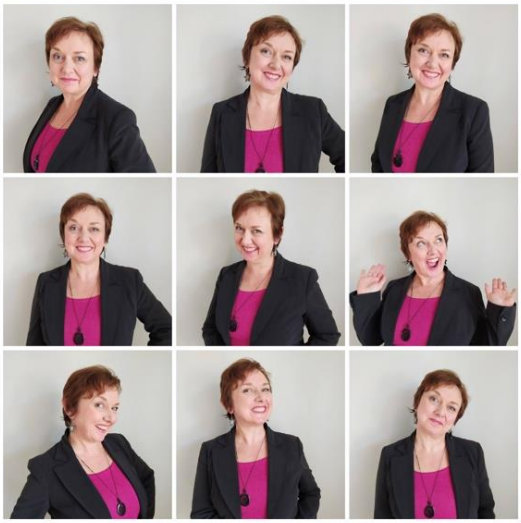
R2,760.00 incl vat

To Book

Please email us with your preferred date attendance dates at: info@velisaafrica.co.za

Please advise if you wish to make a corporate booking for 4 or more from the same Company

Course Presenter Biography



.

Caroline has 25 years' experience in IT systems development, IT service management and Information Governance consulting.

She has worked with over 20 IT Departments in 4 different countries (hot tip: IT is the same *everywhere*). She has been working on POPI compliance and privacy and data protection projects since 2017.

Caroline is certified in **Cyber Incident Planning & Response (CIPR)**

View certification

Please note that Caroline is not a legal practitioner and cannot provide legal advice or legal services.