Moonstone Compliance Incident Response Management Webinar 2022

18 May 2022

Presented by **Andrea de Jongh**

Agenda

Time	Topic	Presenter
10:00 - 10:05	**Opening and Welcome**	Andrea de Jongh
10:05 – 11:30	**Incident response management**	Andrea de Jongh
11:30 – 12:00	**Questions and Answers**	Andrea de Jongh

CONTEXT

- No one is invulnerable to an unauthorized access incident, regardless how mature your Privacy Governance Programme is.
- Always busy compiling our disclosure of evidence bundle for the Information Regulator.
- Always in conversation with the Information Regulator, recording why we may process personal information and what we are doing to keep it save.
- In the absence of a Guideline on how to respond to an unauthorised access incident, we now have two media statements to help us understand what the Information Regulator requires from us.
- **Learnings for today:** understanding why the various phases within a Privacy Governance Programme are important, and having the insight to use the learnings out of each when reacting to an unauthorised access incident

WHY?

- 4IR, drivers of change and coping with hypergrowth
- Building Resilience
- Unconscious incompetence
- A data breach presents a high risk to:
  - legal entities [material (financial e.g., fines, reputational damage, direct and indirect cost)] and non-material [identity fraud leading to loss of goodwill]
  - the rights and freedoms of individuals, has the potential to result in:
    - material (e.g., financial loss e.g., credit card details could have been affected); and
    - non-material damage (e.g., identity theft or fraud if identity card details have been affected in combination with credit card details or banking details)

WHAT IS IT?

- POPIA s22
- The role of human error in personal data breaches must be highlighted, due to its common appearance. Since these types of breaches can be both intentional and unintentional, it is very hard for the data controllers to identify the vulnerabilities and adopt measures to avoid them.

RISK ASSESSMENT

- Consider the nature, sensitivity, and volume of personal data affected:
  - the number of individuals affected?
  - the overall quantity of affected personal data?
  - The risk of combining the types of data breached when processed together – ie identity theft or fraud
- Consider whether the data can be restored after an attack, if not due to poor organisational controls, it would increase the risk if the backup files were affected by the ransomware

WHAT IS CYBERSECURITY?

- Know the hazards before you go in there.
- Cybersecurity has parameters, some we can control, others we cant
- Reasons for increase in attacks:
  - Reprioritisation to move to cloud as a result of the pandemic – work from home, resulting in:
    - Increased opportunity for Personal Information to be compromised;
    - Misinformation and disinformation;
    - Ungoverned online space

WHAT IS CYBERSECURITY?

- Types of cyber threats:
  - Phishing
  - Data breaches
  - Identity theft
  - Malware

UNDERSTANDING CYBERSECURITY

- Malicious users
  - Terrorists
  - Industrial Spies
  - Organised crime groups
  - Cyber bullying

UNDERSTANDING CYBERSECURITY

- Building blocks to cybersecurity
  - Password managers
  - Updated Antivirus
  - Backups
  - Training your employees out of unconscious incompetence into unconscious competence

DATA PRIVACY PROGRAMMES

- **Legal compliance**
  - POPIA
  - PAIA
  - FSP Compliance universe
  - Cybercrimes Act

POPIA – Privacy Governance as your point of departure

Andrea de Jongh

DATA PRIVACY PROGRAMMES

a) Executive buy in
b) Know your data
c) Policy-setting
d) Training
e) Vendor & third-party management
f) Legal compliance
g) Reporting

KNOW YOUR DATA

• POPIA s17 (art 30 GDPR) read with PAIA – you need a record of processing activities, specifically, where in your operation you process personal information

• This will help your governance risk and compliance relating to data, help you take informed risks, and have a record of your processing and level of compliance

Fact finding mission:

- Know where your gaps are;
- If you know what your benchmark is, you will understand whether you are applying the required standards and principles to your processing activities;
- You can't do this if you don't have a clear understanding of where you are processing personal information; and
- What your justification ground(s) is/are

THE CRUX OF POPIA

POPIA

Protection of Personal Information Act

ACT Summary and Preamble

Chapter 1 Definitions and Purpose

Chapter 2 Application Provisions

Chapter 3 Conditions for lawful Processing

Part A Processing of personal information in general

Condition 1 Accountability

Condition 2 Processing limitation

Section 9 Lawfulness of processing

Section 10 Minimality

Section 11 Consent, justification and objection

Section 12 Collection directly from data subject

Condition 3 Purpose specification

Section 4 Lawful processing of personal information

(1) The conditions for the lawful processing of personal information by or for a responsible part are the following:

- **(a) "Accountability",** as referred to in section 8;
- **(b) "Processing limitation",** as referred to in sections 9 to 12;
- **(c) "Purpose specification",** as referred to in sections 13 to 14;
- **(d) "Further processing limitation",** as referred to in section 15;
- **(e) "Information quality",** as referred to in section 16;
- **(f) "Openness",** as referred to in sections 17 and 18;
- **(g) "Security safeguards",** as referred to in sections 19 to 22; and
- **(h) "Data subject participation",** as referred to in sections 23 to 25.

(2) The conditions, as referred to in subsection (1), are not applicable to the processing of personal information to the extent that such processing is:

- (a) excluded, in terms of section 6 to 7, from the operation of this Act; or
- (b) Exempted in terms of section 37 to 38, from one or more of the conditions concerned in relation to such processing.

THE CRUX OF POPIA

Section 11 Consent, justification and objection

(1) Personal information may only be processed if:

a. the data subject or competent person where the data subject is a child consents to the processing;
b. Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
c. Processing companies with an obligation imposed by law on the responsible party;
d. Processing protects a legitimate interest of the data subject;
e. Processing is necessary for the proper performance of a public law duty by a public body; or
f. Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied

(2)

a. The responsible party bears the burden of proof for the data subject's or competent person's consent as referred to in subsection (1)(a).
b. The data subject or competent person may withdraw his, her or its consent, as referred to in subsection (1)(a), at any time: Provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information in terms of subsection (1)(b) to (f) will not be affected.

KNOW YOUR DATA

Identifying your processing activities and Legal Compliance

- Identify every processing activity in the organisation where personal information is collected
  - Processing activities where no personal information is collected do not fall within the ambit of POPIA.

- **Identify the legal justifications for the processing of personal information within each activity (section 11).**
  - If the organisation cannot justify (per the grounds provided in section 11)
  - why it is processing the personal information,
  - it must stop processing immediately.

KNOW YOUR DATA

Identifying your processing activities and Legal Compliance

- Identify every processing activity in the organisation where personal information is collected
  - Processing activities where no personal information is collected do not fall within the ambit of POPIA.

- **Identify the legal justifications for the processing of personal information within each activity (section 11).**
  - Where the organisation has identified any special personal information is collected within the processing activity:
    - ensure that such processing adheres to the conditions listed in sections 26 to 33, as applicable.
  - Where the organisation has identified that personal information of a child is processed is collected within the processing activity:
    - ensure that such processing adheres to the conditions listed in sections 34 and 35, as applicable.

KNOW YOUR DATA

Data mapping, forms and documenting processing activities

- Document and data map each of the processing activities
  - It is important to identify and be able to demonstrate to the Information Regulator where the personal information is collected from, with whom it is shared and how it will be stored.

- Identify the processing activities in your organisation that requires data subjects to complete or fill in a form
  - Forms include hard copies and online versions.

- Evaluate and assess each data field on the form to establish whether the organisation has a legal justification for the collection of the personal information requested in each field
  - This process will help to simplify your forms, as the organisation must refrain from requesting personal information which is not relevant to the performance of the services rendered by the organisation.

KNOW YOUR DATA

Inherent risk ratings

- Perform an inherent risk rating on each processing activity, by looking at:
  - Factors such as the volume of Personal Information processed; whether the Personal Information is valuable; will there be a disruption to the business if the Personal Information is lost; how easily can the Personal Information be recovered etc.; and
  - Risk criteria, namely the terms of reference against which the significance of risk is evaluated, e.g.
    - Risk criteria are based on organizational objectives, and external context and internal context; and
    - Risk criteria can be derived from standards, laws, policies and other requirements.

KNOW YOUR DATA

Inherent risk ratings

- Risk ratings are usually conducted according to a “likelihood” and “impact” scoring model, where the combined score provides the inherent risk rating.
- The aforementioned is done to identify which processing activities pose the highest risk for the organisation
- These are the risks that the organisation will have to address first.

KNOW YOUR DATA

Risk Criteria

Risk criteria derived from an external context refers to the external environment in which the organization seeks to achieve its objectives

- **External context can include the following:**
  - the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
  - key drivers and trends having impact on the *objectives* of the organization;
  - relationships with, and perceptions and values of, external stakeholders **.**

KNOW YOUR DATA

Risk Criteria

Risk criteria derived from an internal context refers to the internal environment in which the organization seeks to achieve its objectives

- **Internal context can include:**
  - governance, organizational structure, roles and accountabilities;
  - policies, objectives, and the strategies that are in place to achieve them;
  - the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
  - information systems, information flows and decision-making processes (both formal and informal);
  - relationships with, and perceptions and values of, internal stakeholders;
  - the organization's culture;
  - standards, guidelines and models adopted by the organization;
  - form and extent of contractual relationships.

KNOW YOUR DATA

Risk Treatment

What is it?

- Risk treatment is the process to modify risk and can involve:
  - avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
  - taking or increasing risk in order to pursue an opportunity;
  - removing the risk source;
  - changing the likelihood;
  - changing the consequences;
  - sharing the risk with another party or parties (including contracts and risk financing);
  - retaining the risk by informed choice.

- Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

- Risk treatment can create new risks or modify existing risks.

KNOW YOUR DATA

Residual Risk

What is it?

- Residual risk is the risk remaining after risk treatment
  - Residual risk can contain unidentified risk.
  - Residual risk can also be referred to as “retained risk”.

KNOW YOUR DATA

Non-conformances & Solutions (Regulatory Risk Register)

Identify which remedial steps will be implemented to address the non-conformances. There are four types of control measures:

1. Directive Control Measure

Directive controls provide guidance on how to prevent a risk or loss. It is the simplest form of an internal control system, but also the easiest to implement, e.g. Policies, Procedures and Training Sessions

2. Preventative Control Measure

Preventative controls are designed to prevent the materialisation of loss or risk before they occur, e.g. separation of duties, various sign off and approval systems, insurance measures and reporting.

3. Detective Control Measure

Detective controls are designed to discover the source of an error or irregularities and to correct it accordingly. Detective controls can assist to prevent small problems from becoming major problems, e.g. the regular reviewing and updating of systems.

4. Corrective Control Measure

Corrective controls aim to remedy problems that can be systematically corrected, e.g. additional training or gradual changes in procedures.

KNOW YOUR DATA

Non-conformances & Solutions (Regulatory Risk Register)

- The remedial steps is to:
  - ensure that the processing activity is compliant with POPIA, the non-conformances must be brought in line with the conditions for lawful processing
  - incorporate the 8 conditions for lawful processing

KNOW YOUR DATA

Non-conformances & Solutions (Regulatory Risk Register)

- Starting with the processing activities which scored the highest risk ratings during activity 10, measure each data mapped processing activity against the conditions for lawful processing stipulated in POPIA, and note the non-conformances in your Regulatory Risk Register.
  - By measuring your processing activities against the conditions for lawful processing, the organisation is establishing whether its processing activities are in fact POPIA compliant or not.
  - Processing activities with a “lower” risk rating can be dealt with after the processing activities with a “higher” risk rating have been fully addressed.
- Identify which remedial steps will be implemented to address the non-conformances.
  - To ensure that the processing activity is compliant with POPIA, the non-conformances must be brought in line with the conditions for lawful processing through the identification of remedial steps which incorporates the conditions for lawful processing.

KNOW YOUR DATA

Non-conformances & Solutions (Regulatory Risk Register)

- Starting with the processing activities which scored the highest risk ratings:
  - measure each data mapped processing activity against the conditions for lawful processing stipulated in POPIA: and
  - note the non-conformances in your Regulatory Risk Register.
- By measuring your processing activities against the conditions for lawful processing, the organisation is establishing whether its processing activities are in fact POPIA compliant or not.
- Processing activities with a “lower” risk rating can be dealt with after the processing activities with a “higher” risk rating have been fully addressed.
- Identify which remedial steps will be implemented to address the non-conformances:
  - to ensure that the processing activity is compliant with POPIA;
  - the non-conformances must be brought in line with the conditions for lawful processing;
  - through the identification of remedial steps which incorporates the conditions for lawful processing.

KNOW YOUR DATA

Non-conformances & Solutions (Regulatory Risk Register)

- Set out the remedial steps in a project timeline, according to which the proposed remedies will be implemented.
  - Assign a responsible person and a due date by which the remedial steps must be implemented.

- Monitor the effectiveness of the remedies implemented.
  - Propose and implement alternate remedies if the current remedies are inefficient

KNOW YOUR DATA

Policy Setting

- Draft and implement an Information Security Management Policy. Where there is an existing Information Security Management Policy, review the content to ensure that it is in line with
  - Refer to ISO Standards 27001 (the Requirements for setting up the information security management system (“ISMS”)) and 27002 (the Code of Good Practice for ISMS) for guidance.

  - Ensure that the Information Security Management Policy addresses the organisation’s incident management procedure, information security risk assessments, information asset registers and information security assessments.

KNOW YOUR DATA

Classic Information Security Management System (“ISMS”) Roadmap (27001)

- **Establishing the context:**
  - Initiating, scope & policy – section 4
  - Leadership – section 5
- **Planning – section 6:**
  - Risk methodology & acceptance
  - Risk assessment
  - Risk treatment & Statement of Applicability
- **Supporting Activities:**
  - Implementation – section 7
  - Training & Awareness – section 8
- **Performance Evaluation – section 9:**
  - Monitor, Review, & Internal Audit
  - Continual Improvement
  - Certification and External Audit
  - Run ISMS

KNOW YOUR DATA

Regarding the Performance Evaluation (Section 9 ISO 27001)

- **Relevant Standards:**
  - ISO 19011 – Guidelines for auditing management systems
    - ISO 27007 – Guidelines for ISMS auditing
    - ISO 27008 – Guidelines for auditing information Security Controls

- **How to perform an audit?**
  - ISO 27001 Management System Standard:
    - Utilise competent auditors
    - Auditor audit - Organisation auditee

CYBERCRIMES ACT

The commencement date of the Cybercrimes Act

The President of South Africa has proclaimed the Cybercrimes Act commencement date of certain sections to be 1 December 2021.

- **Chapter 1** | Definitions and Interpretations
- **Chapter 2** | Cybercrimes (Parts I to V only)
- **Chapter 3** | Jurisdiction
- **Chapter 4** | Powers to investigate, Search, Access or Seize (except sections 38(1)(d)-(f), 40(3)-(4), and (41-44))
- **Chapter 7** | Evidence
- **Chapter 8** | Reporting Obligations and Capacity Building (except section 54)
- **Chapter 9** | General Provisions (except sections 11B-D, and 56A(3)(c) - (e) of Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007, in the Schedule of laws repealed or amended in terms of section 58).

CYBERCRIMES ACT

Chapter 2 | Cybercrimes

[commencement date of Chapter 2 (excluding Part VI): December 2021]

- **Part I** | Cybercrimes
- **Part II** | Malicious Communications
- **Part II** | Attempting, Conspiring, Aiding, Abetting, Inducing, Inciting, Instigating, Instructing, Commanding or Producing to Commit Offence
- **Part IV** | Compete Verdicts
- **Part V** | Sentencing
- **Part VI** | Orders to Protect Complaints from the Harmful Effects of Malicious Communications

CYBERCRIMES ACT

Section 17 | Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit offence

Any person who unlawfully and intentionally -

1) Attempts;
2) Conspires with any other person; or
3) Aids, abets, induces, incites, instigates, instructs, commands or procures another person, to commit an offence in terms of Part I or Part II of this Chapter, is guilty of an offence and is liable on conviction to punishment to which a person convicted of actually committing that offence would be liable

CYBERCRIMES ACT

Section 2 | Unlawful Access

(1). Any person who unlawfully and intentionally performs an act in respect -

a. A computer system; or
b. A computer data storage medium, which places the person who performed the act or any other person in a position to commit an offence contemplated in subsection (2), section 3(1), 5(1) or 6(1), is guilty of an offence.

CYBERCRIMES ACT

ACT Summary and Preamble

Chapter 1 | Definitions and Interpretation

Chapter 2 | Cybercrimes

Part 1 | Cybercrimes

Section 2 | **Unlawful access**
Section 3 | **Unlawful interception of data**
Section 4 | **Unlawful acts in respect of software or hardware tool**
Section 5 | **Unlawful interference with data or computer program**
Section 6 | **Unlawful interference with computer data storage medium or computer system**
Section 7 | **Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device**
Section 8 | **Cyber fraud**
Section 9 | **Cyber forgery and uttering**
Section 10 | **Cyber extortion**
Section 11 | **Aggravated offences**
Section 12 | **Theft or incorporeal property**

BUSINESS BEST PRACTICE TO PREVENT CYBERSECURITY BREACH

- Build and practice good cyber hygiene (preventative measure)
- Protect access to assets (protect business value)
- Protect email domain (prevent phishing attacks)
- Build disaster recovery plan (mitigate cyber risk)
- Build culture of cybersecurity (support a protected environment)

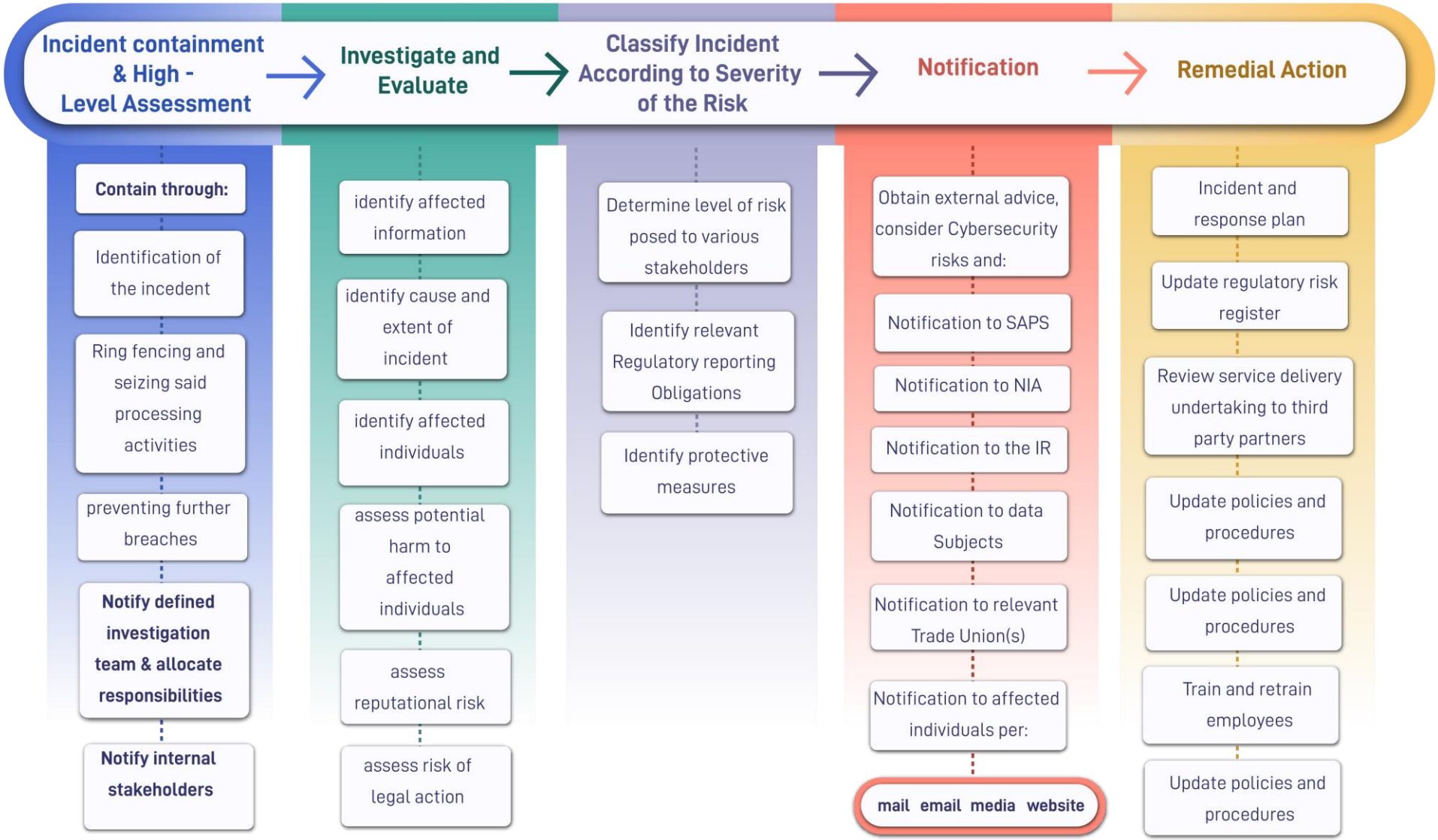
CYBERSECURITY PRO-ACTIVE BEHAVIOUR

- Keep it lean
- Keep your privacy settings on when browsing
- Practice good internet hygiene, use a secure VPN connection
  - Where the private network connects to the world, don’t conduct your banking on an open network.
  - Don’t be tricked into downloading malware
- Password management
- Be mindful of who you meet online
- Keep updated with antivirus programme, provides vital level of security

CYBERSECURITY PRO-ACTIVE BEHAVIOUR

- Understand what your responsibilities are flowing from your Compliance Universe
  - What do you need to report to whom in the event of a breach; and
  - When does your reporting obligation arise?
- Ensure your cybersecurity programme contains sufficient controls to ensure your Compliance Universe responsibilities are integrated and can be met with ease:
  - POPIA (Information Regulator)
  - Cybercrimes Act (SAPS & NIA)
  - Scope of Financial Services Legislation (FSCA)
  - Scope of Registered Credit Providers (Credit Regulator)
  - SARS
- Train your team and colleagues
- Have your service providers in place
- Practice your process – have a Dry-run
- Update your Regulatory Risk Register

There is an Incident



THERE WAS AN INCIDENT

Crux given the two media statements issued by the Information Regulator:

- The need for affected data subjects to be informed early about any security compromise on their personal information to be able to take the necessary preventative action against wrongful use of their personal information is crucial.
- The appropriateness of Responsible Party's security measures on integrity and confidentiality of personal information of data subjects in its possession or under its control will be scrutinised.

THERE WAS AN INCIDENT

Information Regulator issued its first Media Statement on 19 March 2022 in response to the breach the Credit Bureaus suffered – the following information had to be included in the POPIA section 22(5) Notification to affected data subjects

- the date that the security compromise occurred;
- the cause of the security compromise;
- details of investigations into the security compromise;
- the extent and materiality of the security compromise;
- interim measures put in place to prevent a recurrence of the security compromise; and
- security measures that the Credit Bureau has put in place to prevent a recurrence of the security compromise.

THERE WAS AN INCIDENT

The Credit Bureaus' section 22(5) POPIA notification allegedly did not provide information listed in the bullets below, for that reason the Information Regulator issued a second Media Statement on 25 March 2022

- sufficient details nor remedy to the people about whom the personal information relates, whose personal information has been compromised;
- critical information that provides assurance on how the matter is managed;
- detail on how the credit bureau will mitigate the subsequent risks;
- information on how the credit bureau will remedy subsequent risks.

THERE WAS AN INCIDENT

In this second Media statement, the Information Regulator went further and directed the Credit Bureau to provide it with a:

- detailed description of the possible consequences of the security compromise and its impact on data subjects;
- advice and recommendations on the measures to be taken by the data subjects to mitigate the potential adverse effects of the security compromise;
- description of the measures that the Credit Bureau intends to take or has taken to address the security compromise
- confirmation that a criminal case has been opened with the SAPS, in terms of the Cybercrimes Act, Act No. 19 of 2020

THERE WAS AN INCIDENT

- It could happen to you (section 22)
- It could happen to your Operator (section 19)
- **What should you do?**
  - Termination date in your Data Sharing Agreement – when?
  - Notification triggers
  - Right to be kept informed
- **The letters**
  - What should they say? (there are helpful toolkits, and the Media statement from the IR re the Credit Bureau)
  - To whom should they be sent? (section 22)

THERE WAS AN INCIDENT

- There was a data breach incident between *[Date] and [Date].*
- Details of type of breach in your systems
- The data accessed may have included the following types of personal information:
  [List the types of personal information breached]
- The identity of the unauthorised person who may have accessed or acquired the personal information is:
  [If known to the responsible party, declare the identity of the unauthorized person(s)]
- As a result of this breach, below are description(s) of the possible consequence(s) of the security compromise:
  [List the possible consequence(s) of the security compromise]
- You are doing the following to address the security compromise:
  [List the remediation actions that the organisation is performing]
- As per best practice industry standards, you recommend that your data subjects do the following:
  [List the remediation actions that the data subject/customer has control over e.g. change password]

- Inform the data subject that you have notified the Information Regulator ito s22(5) of POPIA.
- Inform the Information Regulator that you have already notified your data subjects ito s22 of POPIA and attach proof.

THEREFORE, DRAFT TWO LETTERS TO START WITH

- Undertake that you will notify the data subjects and the Information Regulator if there are any significant developments.
- If either party have questions regarding the notification, they should contact your Information Officer, include the contact details [IO email address]
- Letter sent under name and title of your Information Officer.

CYBERSECURITY RECOVERY

- Objectives
- Planning and commitment to resources
- Layered protection
  - Implement Tools and Controls
  - Planning for recovery
  - What are the processes and priorities
  - Proper communication channels to prevent brand damage and compliance with your compliance universe
  - Document everything to ensure learning from the experience and continuity

GROUP SUPPORT & MONITORING

- It is a principle-based programme
- It is an organic process
- Don’t mark your own homework

Closing and Questions

Andrea de Jongh

Thank you for your time in viewing this presentation

Andrea de Jongh

Privacy Governance Specialist

adejongh@moonstonecompliance.co.za

MOONSTONE
COMPLIANCE AND RISK MANAGEMENT