MOBIUS
CONSULTING
Actualising change

CYBER SECURITY AND PRIVACY INCIDENT RESPONSE

IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

Information Security related incidents are exponentially rising as organisations face ever-changing threats and increasing risks, ranging from accidental user errors, sophisticated cyber-attacks and disclosure of personally identifiable information.

Most organisations are not equipped to respond to incidents, which often have an adverse impact on their reputation, business operation and regulatory compliance.

Added to this is the reliance on external parties and cloud service providers to support their information processing activities, increasing the threat landscape and complexities to manage an incident.

Is your organisation ready to respond to an incident, manage its potential consequences and notify the relevant internal and external stakeholders?

The good news is, Mobius is perfectly positioned to help your organisation with your response process to better Identify, Protect, Detect, Respond and Recover from an incident.

WHY MOBIUS?

Depending on the severity, various business functions will be required to get involved in the management of the incident, including public relations, legal, business management, information technology, business continuity management.

Additionally, external involvement may include insurers, business partners, service providers, media, and notification to the applicable regulators.

The Mobius approach to Cyber Security Incident Response considers all stakeholder requirements, including Privacy regulators and the Third Parties that will be part of responding to the incident. The processes we help to develop are aligned to the NIST Cyber Security Framework and cover the phases of: **Identify, Protect, Detect, Respond, and Recover.**

HOW?

Our proactive approach aims to make the entire process intuitive, practical to adopt, and aligned to existing processes where possible, enabling you to deal with an incident effectively.

We achieve this by developing an incident response process that applies to your unique situation, which includes identifying the correct internal and external stakeholders to be involved, assisting you in managing the adoption of the process, and finally testing the process to gauge readiness to respond to an incident.

Although you can never be entirely immune to an attack or sensitive data leak, we can help your organisation to be prepared to respond and notify effectively.

PROACTIVE **APPROACH**

TAILORED **INCIDENT RESPONSE**

CYBER ATTACK **READINESS**

NIST CYBER SECURITY **FRAMEWORK**

THE MOBIUS APPROACH
TO CYBER SECURITY INCIDENT RESPONSE

- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

1 PLAN

IDENTIFY AND UNDERSTAND

- Stakeholders and stakeholder groups.
- Existing processes, functions, and detection controls.
- Structures and Cyber Security Incident Response Team (CSIRT) required.
- Cloud and other service providers agreements and responsibilities.
- Privacy, data and other regulator requirements, including business partners and insurer requirements.

OUTCOME
A plan to develop, implement and test incident response.

2 DEVELOP

DESIGN AND DEVELOP

- Incident response processes including roles and responsibilities.
- Practical playbooks based on organisations incident response process.
- Awareness and process training material.
- Communication plans.

OUTCOME
Defined processes, roles and responsibilities, and incident guidelines specific to your organisational structures and functions.

3 ADOPT

IMPLEMENT AND ASSIST

- Create awareness and train all stakeholders.
- Assist with implementation of the process across the organisation.
- Assist with establishing the CSIRT and supporting structure.

OUTCOME
Effective adoption of the Incident Response process and improved response capability.

4 TEST

SIMULATE ATTACK

- Test the entire process by performing a simulated attack.
- Identify incident response improvement areas.
- Provide recommendations for process improvements.

OUTCOME
Assess effectiveness and identify improvement areas.

LET US HELP YOU **IMPROVE YOUR CYBER SECURITY RESPONSE READINESS**

MOBIUS CONSULTING
Actualising change

CONTACT US NOW

Cape Town: +27 21 201 1120 | Johannesburg: +27 10 590 6111 | Email: info@mobiusconsulting.co.za | Website: mobiusconsulting.co.za