communications & digital technologies
Department:
Communications & Digital Technologies
REPUBLIC OF SOUTH AFRICA

ATT: All relevant stakeholders
Decision Document (Wumpus)

RESPONSE OPTIONS & RECOMMENDATIONS

For Infected Actors:
- Containment, Eradication, and Recovery
- Perform trend analysis
- Resilience and need for collaboration

For Infected Technology:
- Perform Vulnerability Audits
- Audit any new systems as a part of continuous improvement
- Post-Incident Activities

For Legislation:
- Open up communication lines with our diplomatic liaisons
- Create a national Critical Infrastructure Protection Program for the future
- Sync recent legislation and business actors' policies
- Proactive and reactive measures

The Threats to the Proposed Responses:
- Economic failure/disruptions
- Civil Unrest
- Armed response backlash
- Disruption of frontline services
- COVID variant (Theta)

Executive Summary:

There is a need to take immediate action in light of recent Ransomware attacks, which have exposed the deficiencies of the current system.

Steps for discussion:

- Components of recovery
- Auditing
- Legislation and Law enforcement
- Threats to current response options

Response Options and Recommendations Decision Processes:

1. Studying Intelligence Report II.
2. Identify affected areas, partners, and stakeholders.
3. Conceptualise the relationship between aspects mention in point (2).
4. Prioritise important/vulnerable relationships from point (3).
5. Develop potential responses and recommendations.
6. Identify possible threats to responses and propose action(s) for said threats.

Team Wumpus 2021