Kenya Airports Authority (KAA): Cyber Security Upgrade

Introduction

Kenya Airports Authority (KAA) is committed to upgrading its information security posture by developing a policy that aligns with NIST Cybersecurity Framework 2. 0. This initiative has been prompted by the recent incidents of unauthorized data breaches, specifically a cyber-attack by the hacking group Medussa; which compromised the KAA's network security and exposed sensitive information.

1) Identify (ID):

- **Asset Management:** document, classify and prioritize critical assets; based on ISO 27002, Annexure A: Physical, People, Technology, Operations, and other essential infrastructure
- **Business Environment:** Identify all the stakeholders and document the process (SOPs) involved in the affected system
- **Governance:** Monitor and review policies, controls and strategies that serve the KAA's critical systems
- **Risk Assessment:** Consider assets / issues: when identifying, evaluating and analyzing risks associated with unauthorized access and data breaches
- **Risk Management Strategy:** Develop strategies for risk treatment tailored to suit KAA's specific needs

2) Protect (PR):

- **Identify Management and Access control:** Implement strong identification, authentication and authorization measures to prevent unauthorized access

- **Awareness Training:** Perform role - based cyber security awareness training to ensure that all the interested parties and stakeholders uphold best practices that safeguards KAA's critical and valuable assets
- **Data Security:** Encrypt sensitive data and ensure that it adheres confidentiality, integrity and availability facets
- **Information Protection Processes and Procedures:** Establish a secure policy, through which audits (internally or externally) and updates are frequently conducted
- **Maintenance:** Conduct regular reviews and updates of KAA's assets and issues
- **Protective Technology:** Ensure that the KAA has a list of devices, software and applications that are only authorized for use

3) Detect (DE)

- **Security continuous monitoring:** Ensure constant monitoring to detect anomalies and potential breaches in real-time
- **Detection process:** Outline a clear process of detecting and analyzing potential adverse events promptly for appropriate response

4) Respond (RS)

- **Response planning:** Develop an incident response plan to conveniently categorize and prioritize breaches before escalation
- **Communications:** Utilize a customized communication map for reporting and managing incidents
- **Analysis:** Analyze and evaluate real-time breaches to determine the source and scope
- **Mitigation:** Implement controls to contain, and lessen the impact of security incidents; ensuring minimal disruption of operations
- **Improvements:** Update incident response plan from the lessons learned as per the past breaches, to enhance future responses

5) Recover (RC)

- **Recovery planning:** Develop and test recovery plans to ensure a secure and prompt restoration of systems after occurrence of breaches
- **Improvements:** Consistently improve the recovery plan as per the lessons learned from past incidents
- **Communications:** Inform all interested parties / stakeholders during the recovery operations to ensure transparency and coordinated efforts

Conclusion: Implementing the NIST CSF 2.0 at Kenya Airports Authority, will ensures a robust security of KAA's network and critical assets. By strictly adhering to these guidelines, we aim at ensuring enhanced confidentiality, integrity and availability of information assets. This will significantly fortify KAA's cyber security posture. This policy is subject to undergo reviewing and updating in order to reflect changes in the overall KAA's information Security posture

Signatory:

John Kimani
Chief Information Security Officer (CISO)
Kenya Airports Authority (KAA).
Date: 6th June, 2024