Ecuitty Bank, Kenya: Information Security Policy

Introduction

Ecuitty Bank Kenya is committed to ensure that its Information Security Management System (ISMS) is at per with the NIST CSF 2.0 Framework. This has prompted by the recent emerging frauds and cyber attacks and has created a need to strength the Cyber Security posture.

1) Identify (ID)

Purpose:

- ***Asset Management:*** Identify, classify all assets in terms of criticality and business value
- ***Business Environment:*** Document the organizational context and the interested parties involved to achieve the business goals
- ***Governance:*** Execute reviewing of policies, strategies and controls to determine their effectivity as per the business objectives
- ***Risk Assessment:*** Consider assets / issues: when identifying, evaluating, analyzing, documenting and reviewing the risks
- ***Risk Management Strategy:*** Determine whether to avoid, mitigate, accept or transfer the risks during the treatment process

2) Protect (PR)

Purpose:

- ***Identify Management and Access control:*** Ensure identities for users, services and hardware are authenticated, monitored and managed. They should be proofed, protected, verified and conveniently conveyed
- ***Awareness Training:*** Perform role - based cyber security awareness training within the organization to ensure that the employees perform their roles with an aim of protecting and improving the cyber security posture

- ***Data Security:*** Ensure that all data is classified, prioritized and conveyed to enhance confidentiality, integrity and availability
- ***Information Protection Processes and Procedures:*** Establish a secure cycle through which the information security policies are audited (internally & externally)
- **Maintenance:** Conduct regular reviews and updates of the organization assets: as well as the overall information security systems
- ***Protective Technology:*** Create and utilize a list of devices, software and applications that are only authorized for use within the organization

3) Detect (DE)

Purpose:

- ***Anomalies and events:*** The Special Operations Center (SOC) team to detect potential adverse events, aiming to determine their source and scope through Cyber Threat Intelligence (CTI) – based analysis
- ***Security continuous monitoring:*** Ensure constant auditing of the information security posture within stipulated intervals (monthly or quarterly)
- ***Detection process:*** Outline the process of detecting and analyzing potential adverse events promptly

4) Respond (RS)

Purpose:

- ***Response planning:*** Involve the relevant third parties in the incident response plan. Validate, categorize and prioritize incidents before escalation as required
- ***Communications:*** Utilize the communication map when responding to incidents
- ***Analysis:*** Analyze incidents to determine the source and scope, for appropriate impact measurements
- ***Mitigation:*** Implement controls to contain, eradicate or lessen the impact of the incidents

- ***Improvements:*** Update response plan from the lessons learned from the incidents that have occurred

5) Recover (RC)

Purpose:

- ***Recovery planning:*** Test business continuity after executing incident response to have an effective disaster recovery plan
- ***Improvements:*** Consistently improve the recovery plan as per the lessons learnt from the incidents
- ***Communications:*** Inform all stakeholders during the recovery operations

Conclusion:

Ecuitty Bank Kenya's information security policy ensures protection of the cyber security posture. By following these guidelines, we aim to maintain information security standards; safeguarding our operations, customers and reputation. This policy will undergo reviewing and updating to reflect changes in the Information Security Management Systems (ISMS)

Signatory:

John Kimani
Information Security Manager
Stoopid Boy Animations Inc.
Date: 3rd June, 2024