ACT EAST AFRICA TREASURY FORUM

Esther Sau, Treasury Accountant, Tullow Kenya B.V

Wycliffe Ogenya, Financial Analyst, Tullow Kenya B.V

Successful fraud mitigation and cyber security strategies

- In law, fraud is a deliberate deception to secure unlawful gain.
- Mitigation, is the effort to reduce severity or painfulness of something.
- Cybersecurity is the practice of protecting systems from digital attacks.

Examining the impact of cyber security on an organisation and risk proofing

- A. **Impact**
- Can be divided into three categories;

i. Financial loss;

a) Theft of corporate information
b) Theft of financial information e.g bank details
c) Theft of money
d) Disruption of trading-inability to transact online
e) Loss of business contract
f) Costs associated with repairing of affected systems and devices

ii. Reputational damage;

a) Loss of customers
b) Loss of sales
c) Reduction in profits
d) Damage relationship with investors and other third parties

iii. Legal consequences

a) Fines and regulatory sanctions – GDPR

B. Risk proofing

a) Train employees in cyber security principles
b) Install, use and regularly update antispyware on every computer

c) Use firewall for internet connection
d) Download and install software updates for your operating systems
e) Make backup copies of business data
f) Control physical access to computer & network components
g) Secure your Wi-Fi networks
h) Require individual user accounts form each employee
i) Limit employee access to data and information
j) Regularly change passwords.

Improved treasury management systems to minimise the risk of fraud

1) Standardized workflows
2) Multi-factor authentication especially for payment approvals
3) Elimination of email and manual steps in approval workflows
4) Treasury-wide audit trails
5) Encryption of all treasury data in transit and at rest
6) Full separation of duties to reduce propensity for internal fraud
7) Central control centres for real-time monitoring of data
8) Independent vendor bank details validation

Enhancing & reviewing governance and internal controls

- An organisation board is accountable to its stakeholders for the framework of standards, processes to secure the organisation against cyber risk through the following;

1) **Cyber security strategy**-based on risk assessment and should address key domains: people, process, technology & compliance.
2) **Enterprise and security architecture** – design IT and security infrastructure to be aligned and support business architecture.
3) **Security audit, intrusion testing** – auditing for the existence & effectiveness of cyber security controls

4) **Regulation &n certification controls**-regulators to pay more attention to cyber breaches and increase fines onerous.
5) **Recovery & continuity plans** – organisation need to develop cyber resilience, a continuum of tested processes in order to respond appropriately to incidents.
6) **Cyber security skills** – organisation to employ staff with adequate skills or ensure security staff acquire and maintain appropriate skills.