The Auditor's Critical Role in Fraud Detection & Prevention

Joseph Mathenge

Discussion Points

- Fraud and Audit - relation
- Audit evolution
- The Fraud Triangle
- Fraud Indicators
- Fraud Control Model
- What next?

Brought to you by
Serianu Cyber-Threat Command Centre

Fraud and Audit

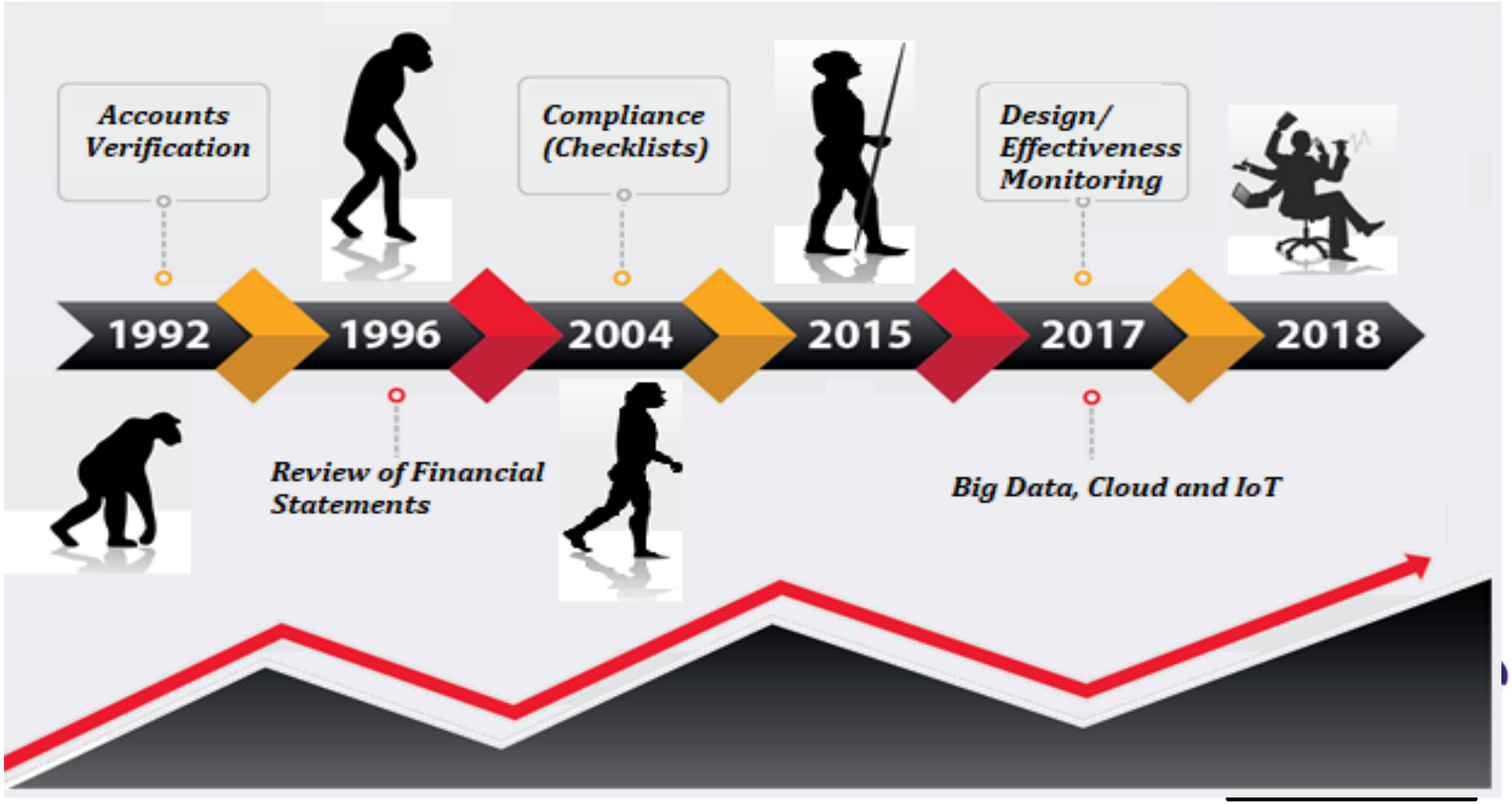
Facts of Fraud

- A challenge every organization faces.
- Hinders performance, wastes scarce resources and inflicts damages.
- Impacts its reputation erodes trust of investors.
- Stakeholders expect that management implement strong control framework

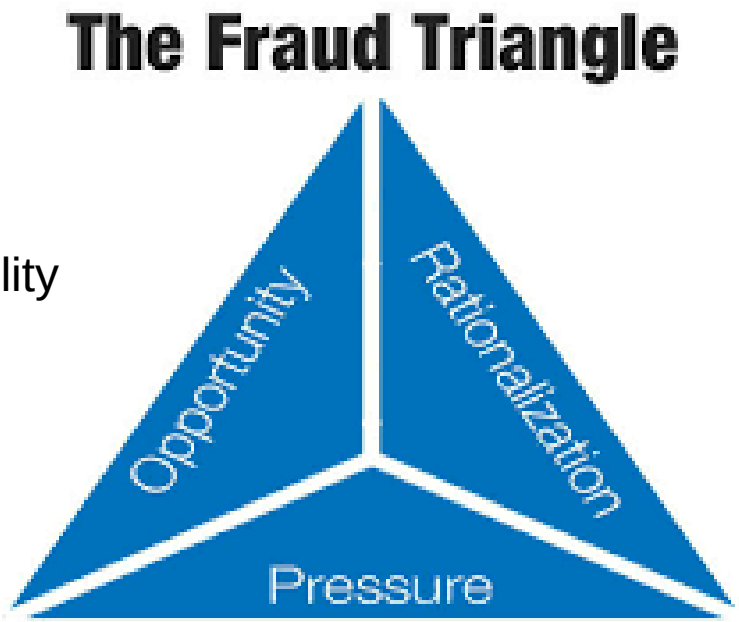
Audit role

- Conduct a fraud risk assessment that identifies an organization's vulnerabilities to internal and external fraud.
- Examine if the organization has implemented fraud prevention controls.
- Examine if the controls are effective.
- Inform and educate all - from employees through to management of strong control environment and that fraud activity will be detected.

Audit evolution



Fraud triangle



Opportunity –
Knowledge and ability to execute

Rationalization –
Justification of committing the act

Motivation or Pressure

Break one and likelihood of fraud reduces significantly

Components of System fraud

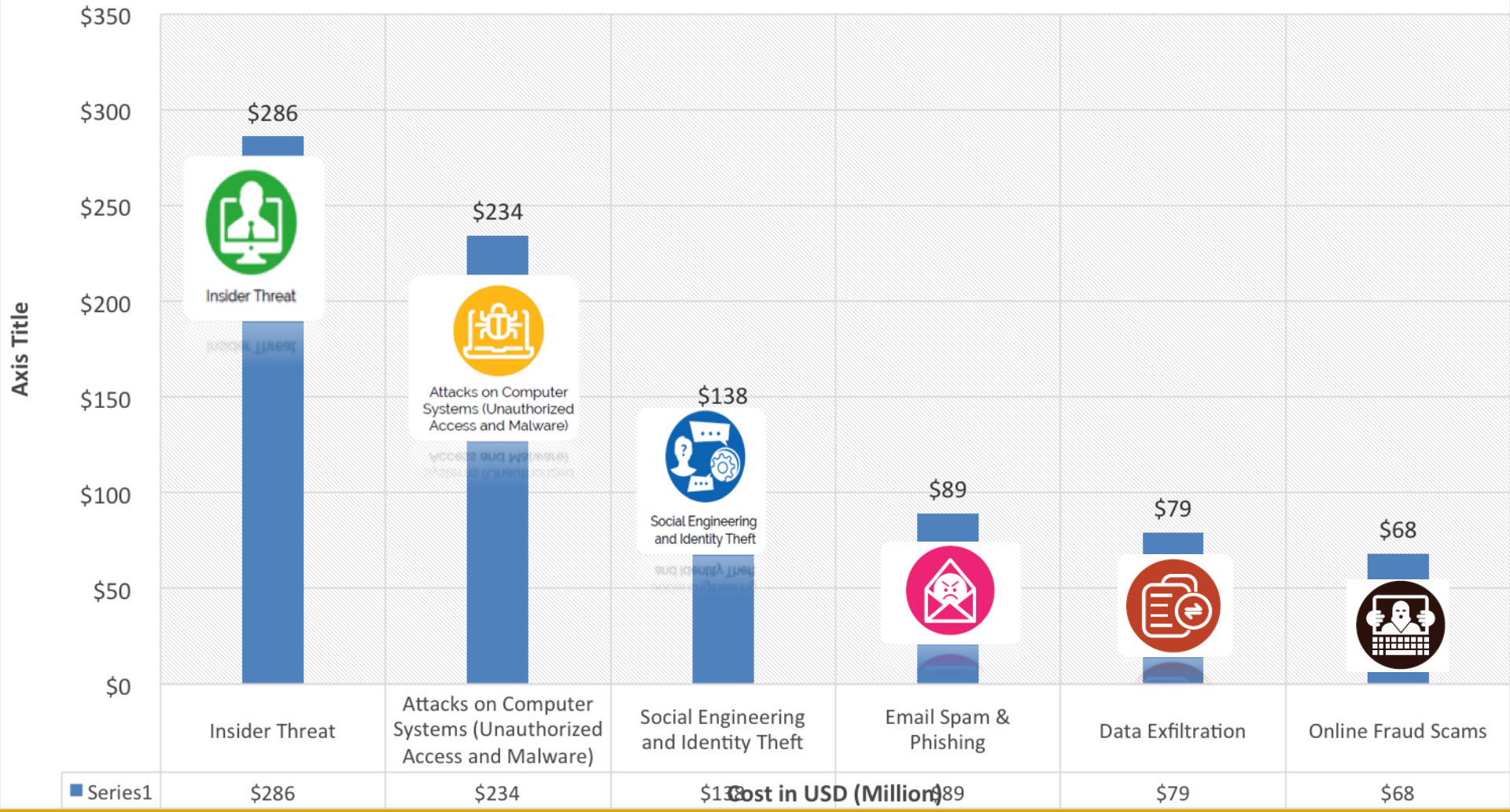
Consider this

- As an avenue to commit fraud
- Tool used to fraud
- Subject of fraud
- Used to cover up fraud

Brought to you by

Serianu Cyber-Threat Command Centre

Cyber-Threat Landscape : Top Attack Methods



Cost of Cyber Crime

Cost of cyber-attacks in Africa

$895m

a year

$537m
Indirect Loss

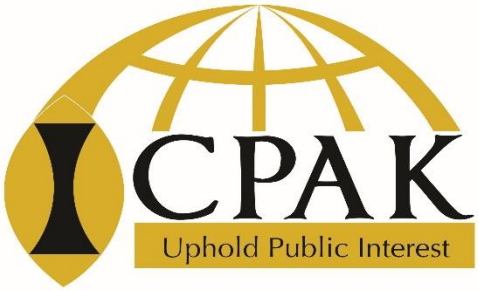
$358m
Direct Loss

Regulator guidance - CBK

CBK Guidance note on Cybersecurity, – Internal Auditor's Mandate

- Continuous review and reporting on cyber risks and controls of the ICT systems
- Assess both the design and effectiveness of the cybersecurity framework.
- Conduct regular independent threat and vulnerability assessment tests.
- Report to the board the findings of the assessments.
- Conduct comprehensive penetration tests.

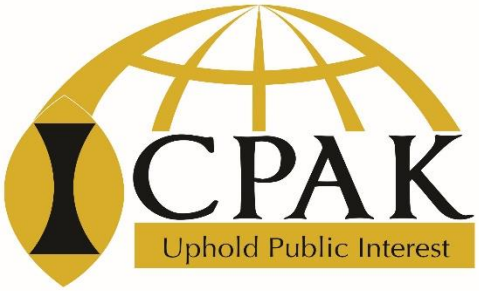
Regulator guidance - SASRA



SASRA Risk Management Guidelines, June 2018– Internal Auditor's Mandate

- Conducting Risk assessments of the ICT systems.
- Review of the ICT Policies, strategy and direction.
- Review of reporting, logging and auditability of the systems.
- Review of adequacy of identification and authentication systems.
- Review of controls in place for protection against malicious malware.

Regulator guidance - IRA



IRA Guidelines on Risk Management and Internal Controls February 2013 – Internal Auditor's Mandate

- Review the design and operational effectiveness of the insurer's individual controls
- Review the reliability and timeliness of escalation processes and reporting systems
- Review the reliability, integrity and completeness of the accounting, financial reporting and management information and IT systems

Can you stop fraud?

- Motivation and rationalization are informed externally
  - Set realistic goals for employees to achieve.
  - A robust and inclusive HR processes that puts humans first.
- A control framework that is dynamic and effective.
- Internal communication and monitoring to examine effectiveness.

Fraud indicators

- Dominant/aggressive personalities or people with too much control
- Resistance to change or a preference for working alone
- Close relationships with suppliers and protectiveness of those relationships
- Generally evasiveness or defensiveness
- Lack of transparency

Fraud Control Model

- The control environment
  - Organizational culture and structure

- Risk Assessment - Weakness or vulnerability identified, likelihood of it occurring and subsequent loss.

- Control activities
  - Policy and Procedures
  - Security (application and Network)

- Information and communication systems
- Monitoring the system

Fraud Control Model

Organizational culture and structure

(a) Does management take undue business risks to achieve objectives?
(b) Does management attempt to manipulate performance measures so they appear more favorable? Does it bend the truth?
(c) Does management pressure employees to achieve results regardless of the methods, or with little concern for those methods?
(d) Is management open and honest with employees about performance and results?

Who is responsible and accountable for Fraud Management in the Organization?

Fraud Control Model

Control Activities – Policies and procedures that provide a basis for individual control techniques

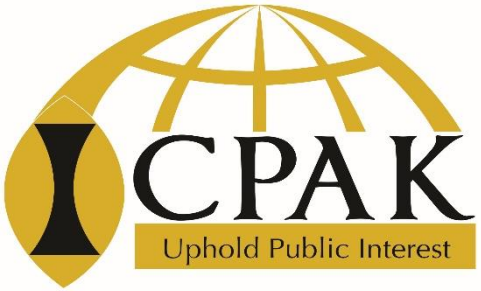
a) *Proper Authorization Processes*
b) *Segregation of Duties*
c) *Adequate Documentation of Transactions*
d) *Physical Controls over Assets and Records*
e) *Independent Internal Checks*

Fraud Control Model

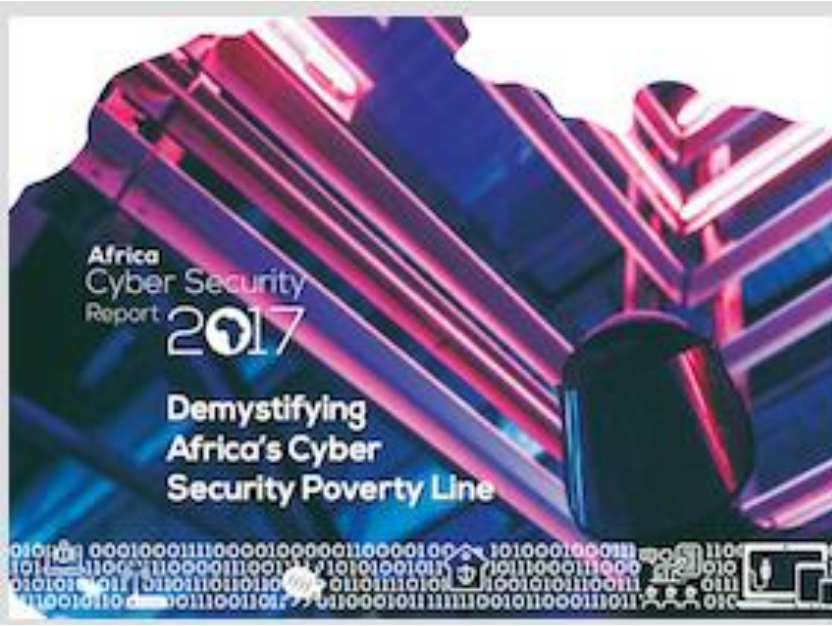
Risk Assessment – where to spend the finite amount of money for maximum effect.

a) *Determine each threats;*
b) *Estimate the likelihood of a loss from each threat;*
c) *Estimate the amount of any loss from each threat;*
d) *Determine what control procedures could be applied;*
e) *Estimate the costs of implementing and maintaining that control;*
f) *Decide whether the control is commercial;*
g) *Implement controls where the cost / benefit assessment is favorable.*

About Serianu



Serianu is a Pan Africa based Cyber Security and business consulting firm. We are an award winning company in the African Cybersecurity sector that helps our customers collect, protect, and analyze critical business information.

Serianu Limited
14 Chalbi Drive, Lavington,
Nairobi, Kenya

Tel: +254 20 240 9294
Mobile: +254 702-847-570
info@serianu.com