Emerging Fraud trends in the current corporate world
Maximising the potential of Digital Forensics
The ICT and fraud convergence
Definitions and context

Definitions

1. **Fraud** is deception intended to result in financial or personal gain.
2. **Computers & the internet** are the two key distinct components of ICT.
3. **Cybercrime** is crime using a computer and the internet as the primary tool to commit fraud.
4. **Traditional frauds schemes** have been enhanced by computers & the internet.
Key statistics and trends
Cybercrime facts for Kenyan organizations; GECs 2016

33% reported having been affected by cybercrime.

61% reported rapid increase in perception of cybercrime.

46%. Said threat coming from both internal and external sources.

*69% Saw IT Department as high risk

*18% Saw HR Department as low risk
Prevalent economic crimes – GECs 2016

Money Laundering
- Kenya: 11%
- Africa: 12%
- Global: 5%

Cybercrime
- Kenya: 32%
- Africa: 28%
- Global: 27%

Bribery and Corruption
- Kenya: 47%
- Africa: 35%
- Global: 24%

Accounting Fraud
- Kenya: 33%
- Africa: 27%
- Global: 18%

Asset Misappropriation
- Kenya: 72%
- Africa: 69%
- Global: 64%

61% experienced economic crime in the past 2 years

Economic Crime in Kenya has risen by 9% points since 2014 with respondents experiencing more asset misappropriation, accounting fraud and bribery & corruption than their global counterparts.
## Prevalent economic crimes – GECs 2016

<table>
<thead>
<tr>
<th>Type of Economic Crime</th>
<th>Likelihood of Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Kenya</td>
</tr>
<tr>
<td>Asset misappropriation</td>
<td>72%</td>
</tr>
<tr>
<td>Accounting Fraud</td>
<td>33%</td>
</tr>
<tr>
<td>Bribery and Corruption</td>
<td>47%</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>27%</td>
</tr>
<tr>
<td>Intellectual Property Infringement</td>
<td>5%</td>
</tr>
<tr>
<td>Money Laundering</td>
<td>5%</td>
</tr>
<tr>
<td>Tax Fraud</td>
<td>7%</td>
</tr>
<tr>
<td>Insider Dealing</td>
<td>7%</td>
</tr>
<tr>
<td>Procurement Fraud</td>
<td>37%</td>
</tr>
<tr>
<td>Mortgage Fraud</td>
<td>7%</td>
</tr>
<tr>
<td>Competition Law/ Anti-Trust Law infringement</td>
<td></td>
</tr>
<tr>
<td>Espionage</td>
<td>3%</td>
</tr>
<tr>
<td>Human Resources fraud</td>
<td>18%</td>
</tr>
<tr>
<td>(recruitment and/or payroll fraud)</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>8%</td>
</tr>
</tbody>
</table>
More on cyber crime and its impact

• Kenya lost Kshs 15 Bn through cyber crime according to 2015 Cyber security report

• Public sector lost more than Kshs 5 Bn followed by the financial services at Ksh 4 Bn;

• Top attacks came from overseas – US, China, etc.

• Kenya has a strong business environment and education system but weak IT physical infrastructure;

• Introduction of cyber security in the Information and Communications Bill 2013.
Cybercrime has hit and remained in the headlines

Cybercrime a growing threat in East Africa

Cybercrime now a "top five" economic threat in East Africa

Kenya lost Sh15bn through cybercrime last year, report says

Cyber crime is Africa's 'next big threat', experts warn

Contents

Key statistics and trends | Digital Forensics | Role of cyber forensics in preventing and detecting fraud

August 2016
Government – Social Engineering

Emerging Fraud trends in the current corporate world

PwC
Private Sector – Bank

- Salami Attack – The case of Hughes Okinda
- Project Swift - RTGS Hack (Westlands bank)
- Project Gikomba – Account Script manipulation
Key risks posed by ICT include....

Function of the computer & internet in crime:

- **As an object** – target of crime where contents are destroyed
- **As a subject** – provide environment to commit crime
- **As a tool** – means of committing crime
- **As a symbol** – offers credibility that is often used to deceive victims

* Relates to 2011 survey
**Offers tremendous appeal to fraudsters**

### Same reward but fewer risks

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not physically present – less likely to be caught or “hurt” during the crime. Also less likely to commit “ancillary” crimes like injuring other people or destroying property</td>
<td></td>
</tr>
<tr>
<td>Less chance that law enforcement can identify the perpetrator or establish where they were when the crime was committed – 79% of Kenya respondents lack confidence in law enforcement</td>
<td></td>
</tr>
<tr>
<td>Perpetrators often in different jurisdiction – more difficult to identify, arrest and prosecute using traditional means</td>
<td></td>
</tr>
<tr>
<td>Current laws are not mature enough to prosecute cybercriminals with sufficient impact.</td>
<td></td>
</tr>
<tr>
<td>Technological advancements are high-paced so too are developments in cybercrimes. Organisations and governments will constantly need to keep updating their responses.</td>
<td></td>
</tr>
<tr>
<td>Preventative controls are much harder to implement for cybercrime than for instance asset misappropriation</td>
<td></td>
</tr>
</tbody>
</table>
Digital Forensics

What is Digital Forensics?

Digital Forensics, Cyber Forensics, Computer forensics – same thing.

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.
The Digital Forensics Process

- Preparation
- Protection
- Imaging
- Examining
- Documentation
Who needs Digital Forensics?

- The victim!
  - Private Business
  - Government
  - Private Individuals
- Law Enforcement
- Insurance Carriers
- Ultimately the Legal system
In the legal world, Evidence is EVERYTHING.
Evidence is used to establish facts
The Forensic Examiner is not biased.
The majority of data is now stored electronically

60 seconds online

- Minicomputer & Mainframe Files
- Web Servers
- Application Service Providers
- E-mail Systems
- Smart phones
- Laptop Computers
- Personal (Home) Computers
- Flash disks
- Optical Media & Tape Backups
- Cloud Storage
**Key characteristics of electronic evidence**

Electronic evidence differs from other types of evidence in that it:

- Is intangible;
- Is volatile;
- Is susceptible to manipulation;
- Can be located in any country in the world;
- Requires examination via the use of computer technology; and
- Tends to be transient in nature.
Role of cyber forensics in preventing and detecting fraud
Although difficult to examine, reducing computer fraud into its basic elements often leads to successful determination.

1. **Lacks traditional paper trail**
2. **Requires understanding of technology used to commit fraud**
3. **Requires understanding of technology on the victim computer**
4. **Often requires use of one or more specialist to assist the fraud examiner**

**Identify culprits**

**Methods of manipulation**

**Means of diversion or conversion of funds**

**Basic elements**

**Inputs** + **Manipulation** + **Outputs** = **=**
What to do then?

3 lines of defense – Governance, Oversight & Operations

They can only be strengthened by technology and not replaced by it.
**Types of Forensic Requests**

- Data Recovery
- Intrusion Analysis
- Damage Assessment
- Suspect Examination
- Tool Analysis
- Log File Analysis or Registry analysis
- Evidence Search (suspect emails/illegal material on company property etc)
Intrusion Analysis

1. Who gained entry?
2. When did this happen?
3. Where did they go?
4. Why the chosen network?
5. How did they do this?
Damage Assessment

What was available for the intruder to see? 
What did he take? 
What did he leave behind? 
Where did he go?
File Recovery

- Deleted Files
- Hidden Files
- Slack Space
- Bad Blocks
- Steganography
- NTFS Streams
Tool Analysis

- What tools were used?
- How were the tools executed?
- What language were they written in?
- File Comparison with Suspect’s File.

Emerging Fraud trends in the current corporate world

PwC

August 2016
Log File Analysis

- Events.
- What Events are monitored?
- What do the event records reveal?
- Firewall/Router/Server log files?
- Modem/FTP/Telnet/RAS
Evidence Search

- Image Files
- Software applications
- Deleted Files
- Hidden Files
- Encrypted Files
- Hidden partitions
- Keyword Search
- Known Remote Access Tools
Proactive Forensic Data Analysis

• Uses sophisticated analytical tools and techniques;
• Computer-based cross-matching;
• Non-obvious relationship identification to highlight potential fraud and misconduct
• Benefits include:
  ◦ Identify hidden relationships;
  ◦ Analyze suspicious transactions;
  ◦ Assess effectiveness of internal controls;
  ◦ Continually monitor fraud threats and vulnerabilities;
  ◦ Consider and analyze thousands of transactions; and
  ◦ Consider a company’s unique organizational and industry issues.
Sample results of proactive data analytics

An example is you’re looking at productions logs and you notice a spike in Hour 4. What questions do you ask?

Investigate?

Ignore?
Sample results of relationship mapping
Do organisations conduct risk assessments?

30% of Kenya respondents have an incident response plan

26% of Kenya respondents say Board members quarterly review organisations ability to deal with cyber incidents

These results are of concern given the rate at which cybercrime is increasing, organisations do not realise that they are a target of cybercrime until long after the damage is done.

Disappointing results in terms of how often Board members within organisations in Kenya and Africa request information regarding the organisations’ state of readiness to deal with cyber incidents.
Build a Cyber crisis management team

- External counsel
- Cyber incident management team
- External service providers
- Law enforcement & government regulators
  - Stakeholders
  - Core team
  - Investigative team
  - Public relations
  - Breach notification
  - Credit monitoring
  - Fraud mitigation
  - Monitor criminal underground
  - Law enforcement
  - Government regulators
Key questions to ponder over

1. Do you really show the right tone at the top in dealing with cyber crime?

2. Does your organisation have an anti fraud policy / strategy including regular training?

3. How do you deal with fraud allegations? How do you deal with fraudsters when you uncover wrongdoing?

4. Is your organisation head truly “cyber savvy” and is your organisation able to detect and investigate cybercrime?

5. Does your organisation undertake regular cyber security assessment?
“As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace”

(Newton Lee, Counterterrorism & Cyber security: Total Information Awareness)