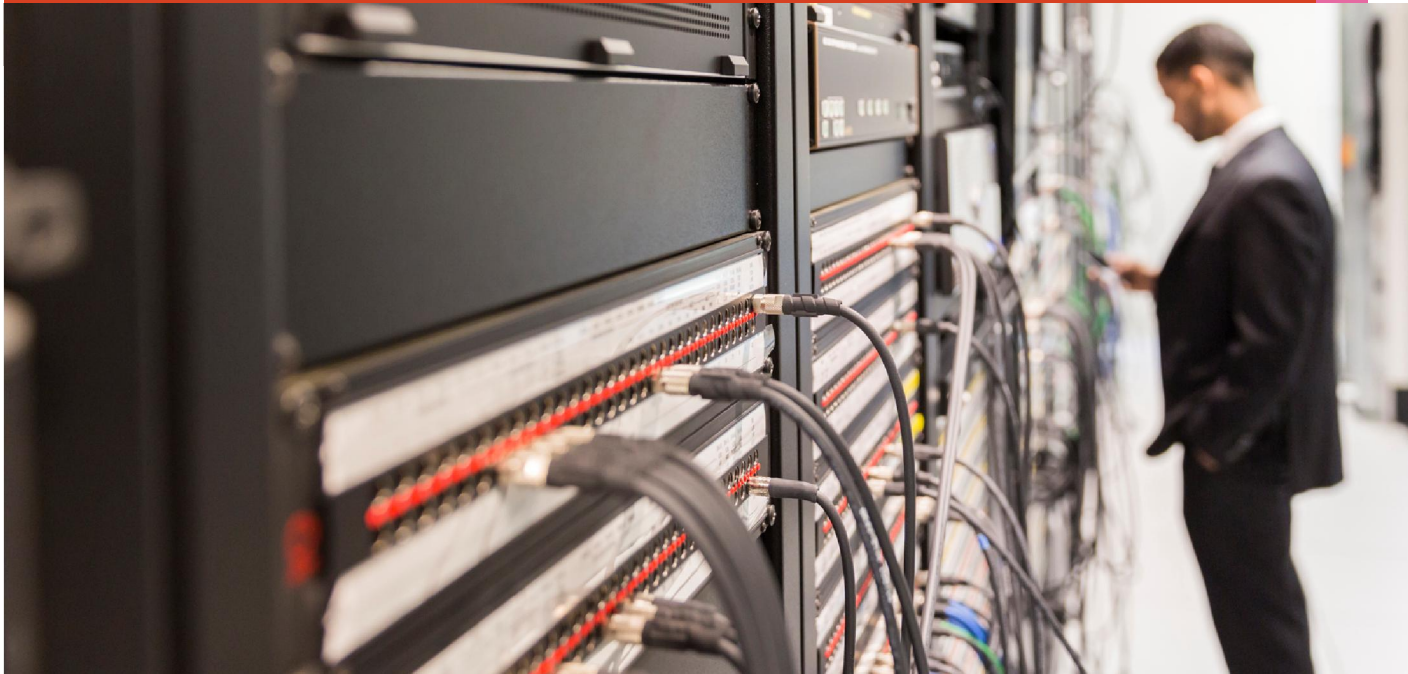


[www.pwc.com/ke](http://www.pwc.com/ke)

# *Emerging Fraud trends in the current corporate world*

## Maximising the potential of Digital Forensics

*Strictly Private  
and Confidential  
August 2016*



**pwc**

# Contents

<b>The ICT and fraud convergence</b>	<b>3</b>
<b>Key statistics and trends</b>	<b>5</b>
<b>Digital Forensics</b>	<b>15</b>
<b>Role of cyber forensics in preventing and detecting fraud</b>	<b>22</b>

# ***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.*

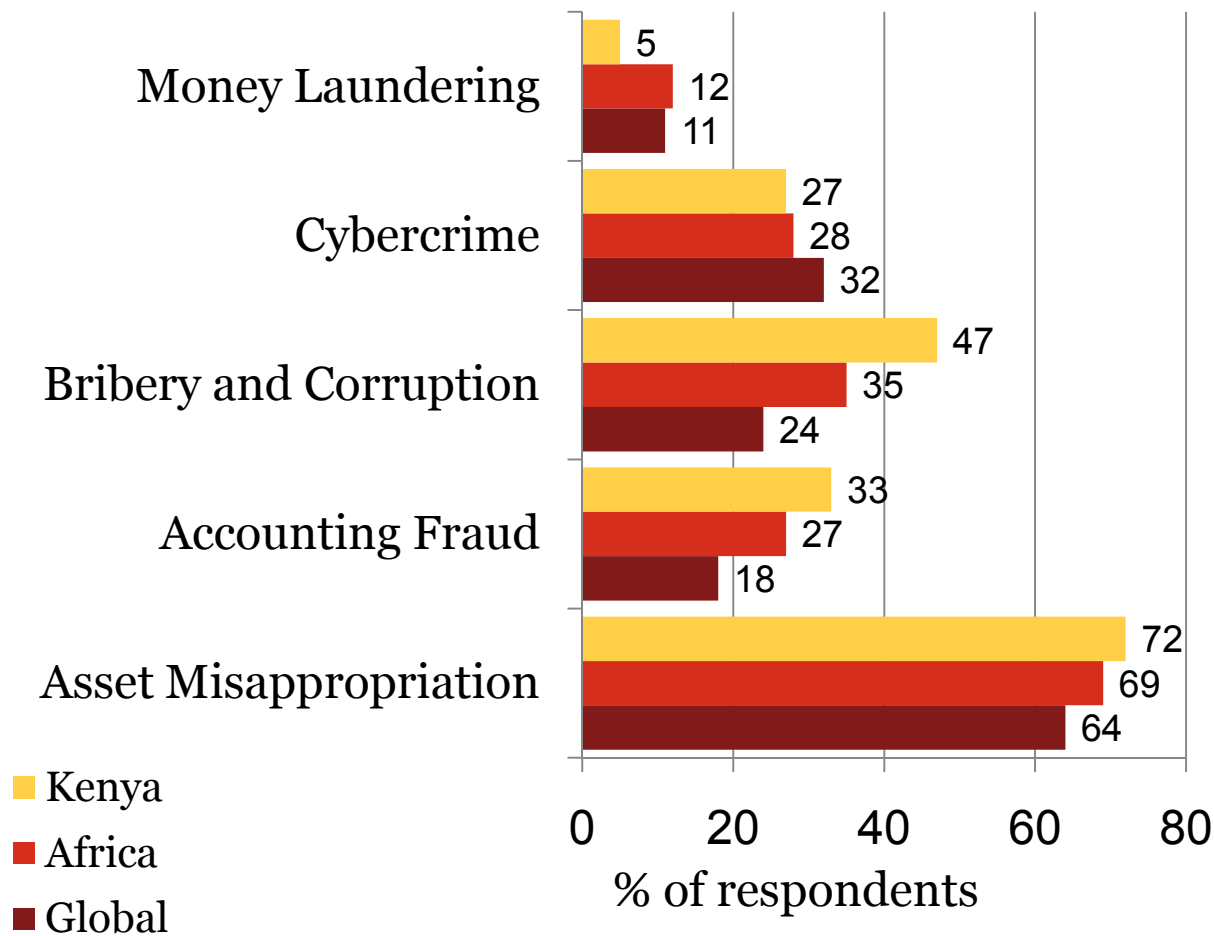
**61%**  
*reported rapid  
increase in perception  
of cybercrime.*

**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



**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

Type of Economic Crime	Likelihood of Occurrence		
	Kenya	Africa	Global
Asset misappropriation	72%	69%	64%
Accounting Fraud	33%	27%	18%
Bribery and Corruption	47%	35%	24%
Cybercrime	27%	28%	32%
Intellectual Property Infringement	5%	6%	7%
Money Laundering	5%	12%	11%
Tax Fraud	7%	7%	6%
Insider Dealing	7%	5%	7%
Procurement Fraud	37%	34%	23%
Mortgage Fraud	7%	5%	6%
Competition Law/ Anti-Trust Law infringement		1%	4%
Espionage	3%	1%	2%
Human Resources fraud (recruitment and/or payroll fraud)	18%	20%	12%
Other	8%	12%	11%



## *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

www.cnbcafrica.com/news/east-africa/2016/01/26/cybercrime-a-growing-threat-in-east-africa-(2)/  
34-001 Imported From Firefox

**EAST AFRICA**

## Cybercrime a growing threat in East Africa

by **Aviwe Mtila** Last Updated: Tue, 26 Jan 2016 11:25:19 GMT



Education around cybercrime and the need for IT security within organisations is needed to protect African businesses. Photo: Flickr.

With cybercrime crippling many businesses across Africa, a recent survey by Kaspersky Lab highlights that 21 per cent of organisations in Kenya are not concerned by the threat.

The survey also shows that education around cybercrime and the need for IT security within organisations is

**DAILY NATION** NEWS BUSINESS COUNTIES SPORTS BLOGS & OPINION LIFE AND

home > business >

## Kenya lost Sh15bn through cybercrime last year, report says

Top attacks on Kenyan systems in 2014 came from the US and China.

WEDNESDAY OCTOBER 28 2015

f 68 t 0 g+ 0 v 0 in 72 p 0 d 0 0.1k



April 2, 2015, 9:25 am.  
Image: By Connected East Africa

**SECURITY**

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

Cybercrime now a Eastern African Cr Kenya loses Sh15 Cyber-crime is Af KenyaCyberSecur 77 C

na.com/stories/201605030697.html

Imported From Firefox

**DAILY NATION** 3 MAY 2016

## Kenya: Walubengo - Hacked Again - Kenya's Cyber Security Must Tighten, Fast

Tagged: East Africa • Kenya • Legal Affairs

Tweet Share Google+ Comment Email More

www.nation.co.ke/news/Cyber-crimes-rise-Kenya/-/1056/2814064/-/aahdxz/-/index.html  
497794-001 Imported From Firefox

**DAILY NATION** NEWS BUSINESS COUNTIES SPORTS BLOGS & OPINION LIFE AND

**BBC** Sign in News Sport Weather iPlayer TV Radio

**NEWS**

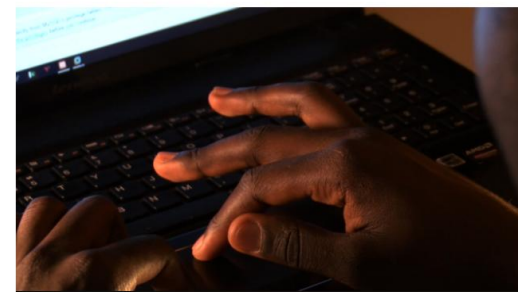
Home UK World Business Politics Tech Science Health Education Entertainment

World Africa Asia Australia Europe Latin America Middle East US & Canada

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

By Tomi Oladipo  
BBC Monitoring Africa security correspondent

© 17 November 2015 Africa



## Government – Social Engineering



## *Private Sector – Bank*

- Salami Attack – The case of Hughes Okinda
- Project Swift- RTGS Hack (Westlands bank)
- Project Gikomba – Account Script manipulation

### **STANDARD BANK CONFIRMS R300M LOST IN CREDIT CARD SCAM**

The scam involved the withdrawal of cash using a small number of fictitious cards at various ATMs in Japan.



## ***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

*Data  
destruction  
& sabotage*

*Unauthorized  
access*

*Internet  
consumer  
fraud*

*Identity  
theft*

*Disclosure of  
confidential  
information*

*Securities  
fraud*

*Loss of  
customer  
confidence*

*Insider  
threat*

*Enhances  
conventional  
fraud*

\* Relates to 2011 survey

## *Offers tremendous appeal to fraudsters*

### **Same reward but fewer risks**

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

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

Perpetrators often in different jurisdiction – more difficult to identify, arrest and prosecute using traditional means

Current laws are not mature enough to prosecute cybercriminals with sufficient impact. Technological advancements are high-paced so too are developments in cybercrimes. Organisations and governments will constantly need to keep updating their responses.

Preventative controls are much harder to implement for cybercrime than for instance asset misappropriation

# *Digital Forensics*



# ***Digital Forensics***

---

## **What is Digital Forensics?**

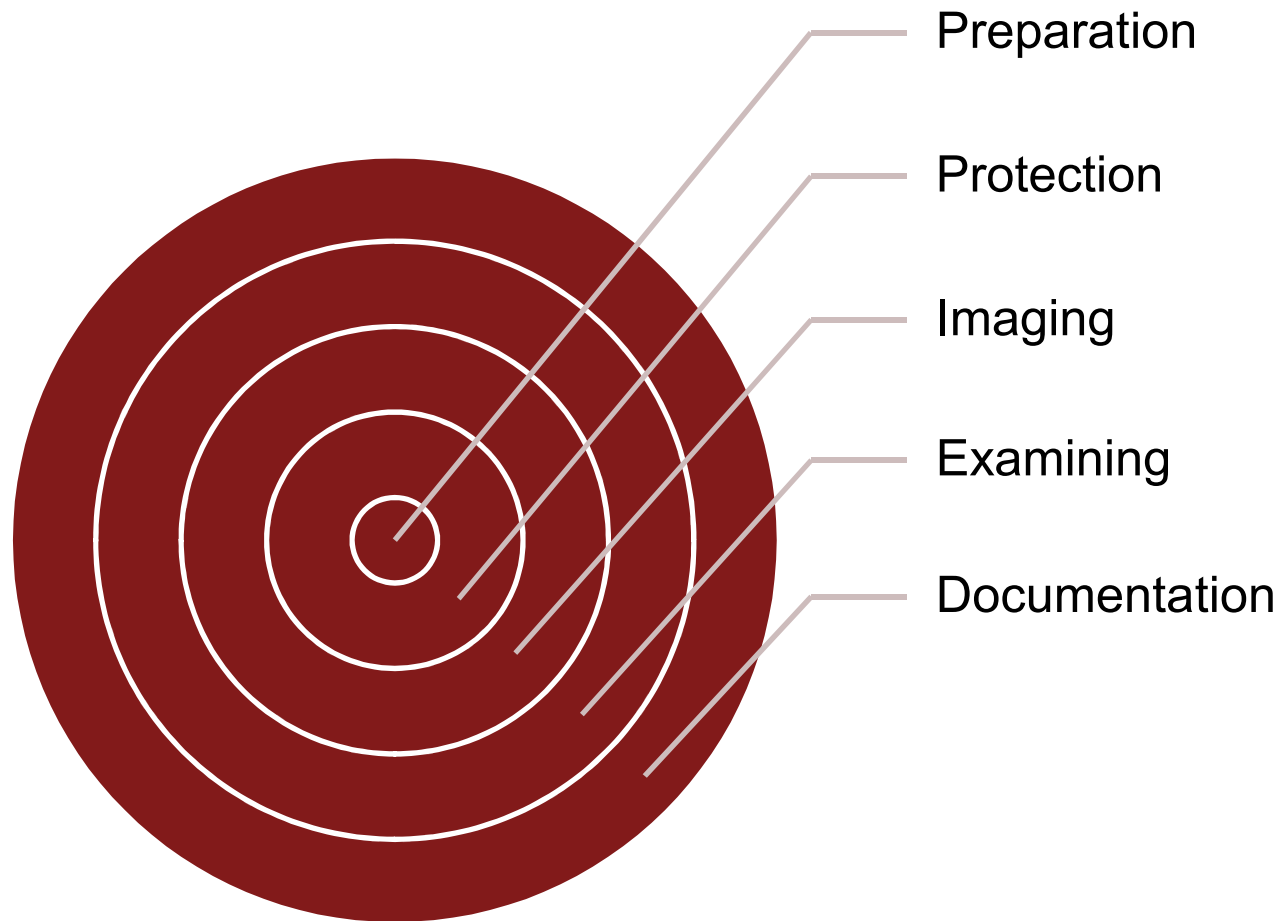
Digital Forensics, Cyber Forensics, Computer forensics – same thing.

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.

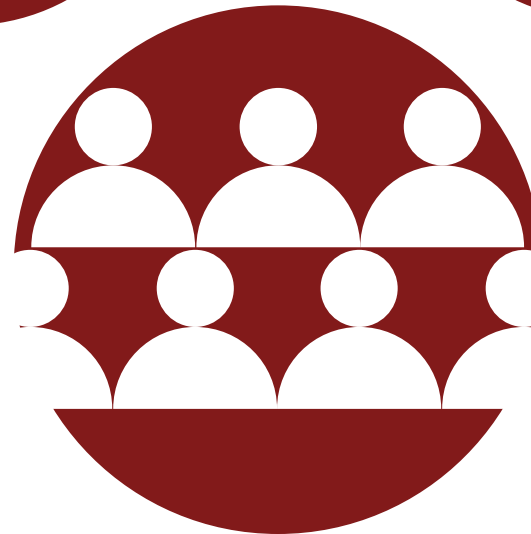


# *The Digital Forensics Process*



## *Who needs Digital Forensics?*

- The victim!
  - Private Business
  - Government
  - Private Individuals
- Law Enforcement
- Insurance Carriers
- Ultimately the Legal system

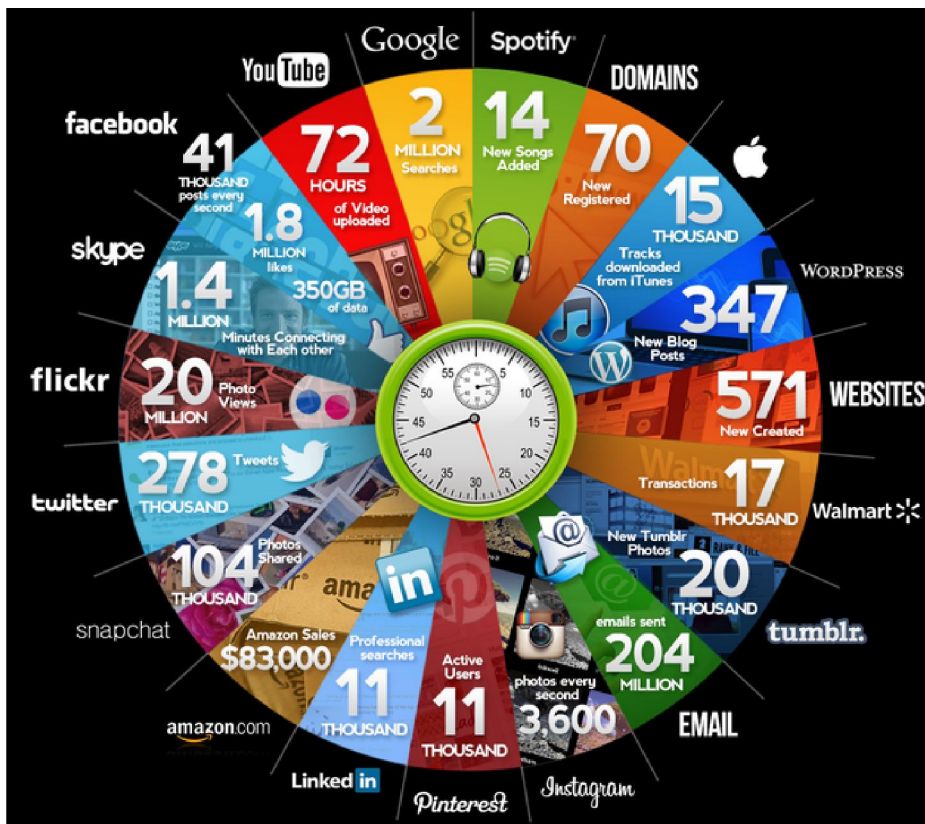


## ***Evidence! Evidence! Evidence!***

- 
- 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***

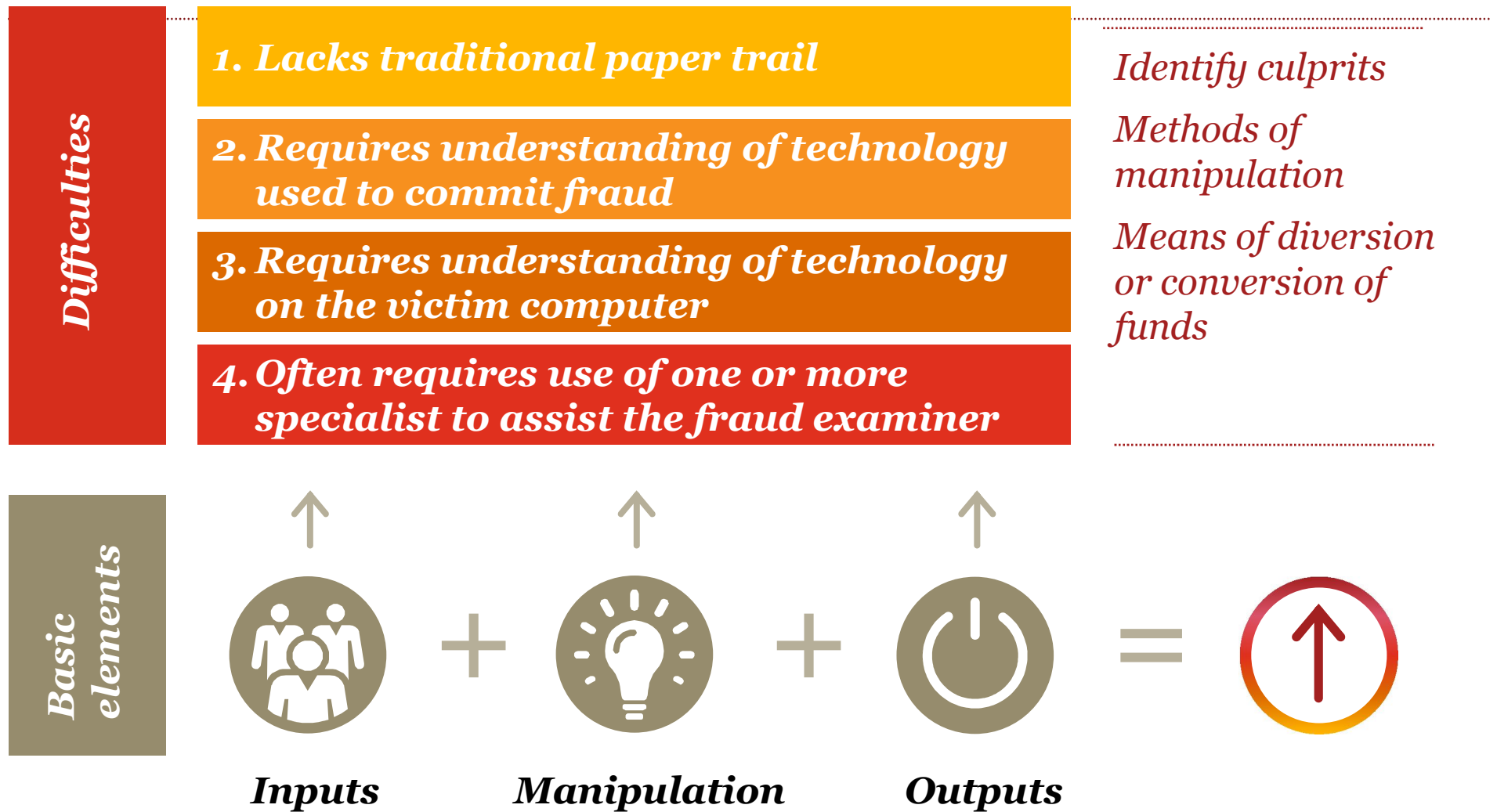
### **Electronic evidence differs from other types of evidence in that it:**

- 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*



## ***What to do then?***

### ***3 lines of defense***

—

Governance, Oversight & Operations

They can only be strengthened by technology and not replaced by it.



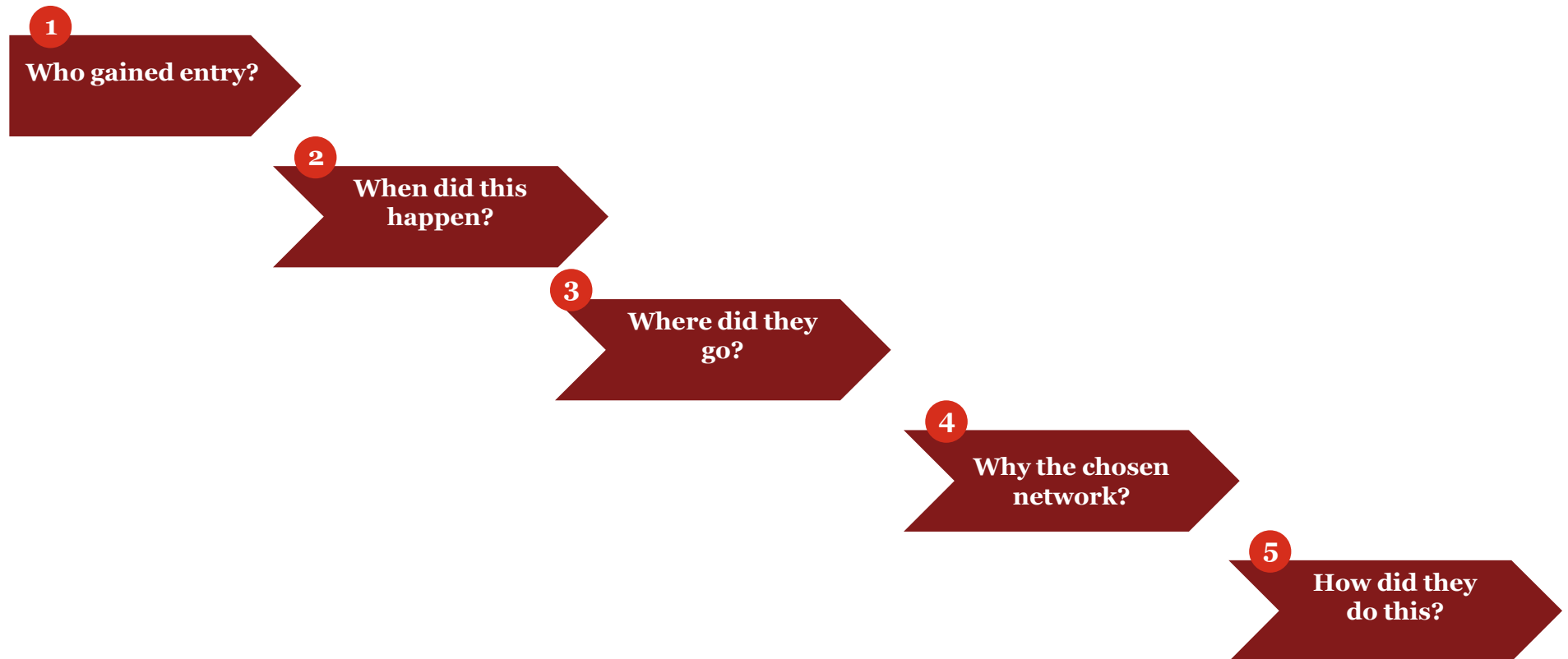


## *Types of Forensic Requests*

- 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)

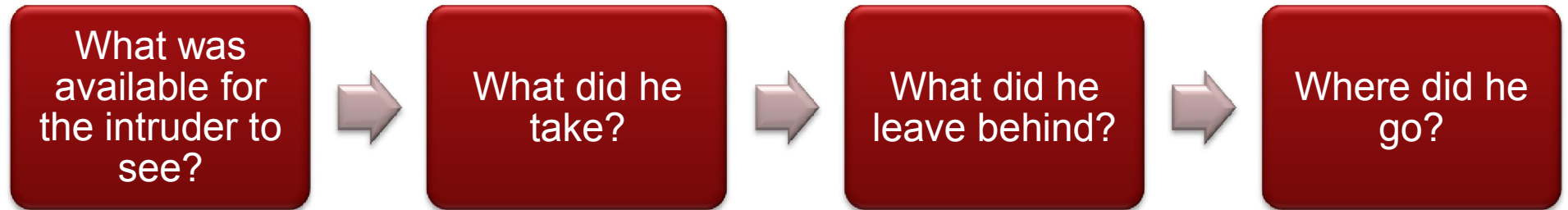


# *Intrusion Analysis*



## *Damage Assessment*

---

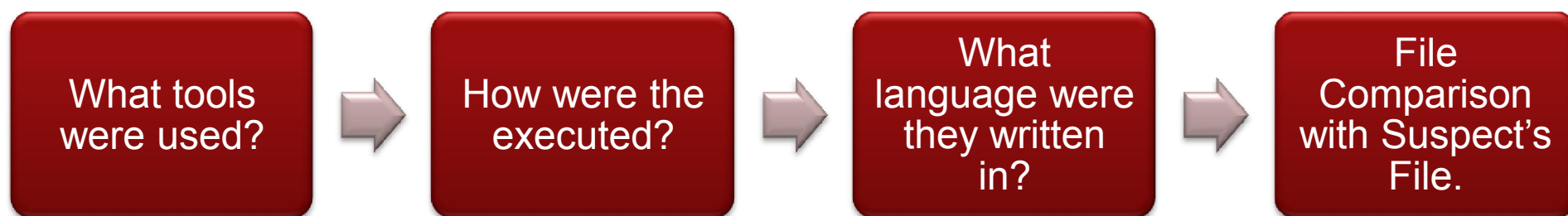


## ***File Recovery***

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

## *Tool Analysis*

---



## *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***

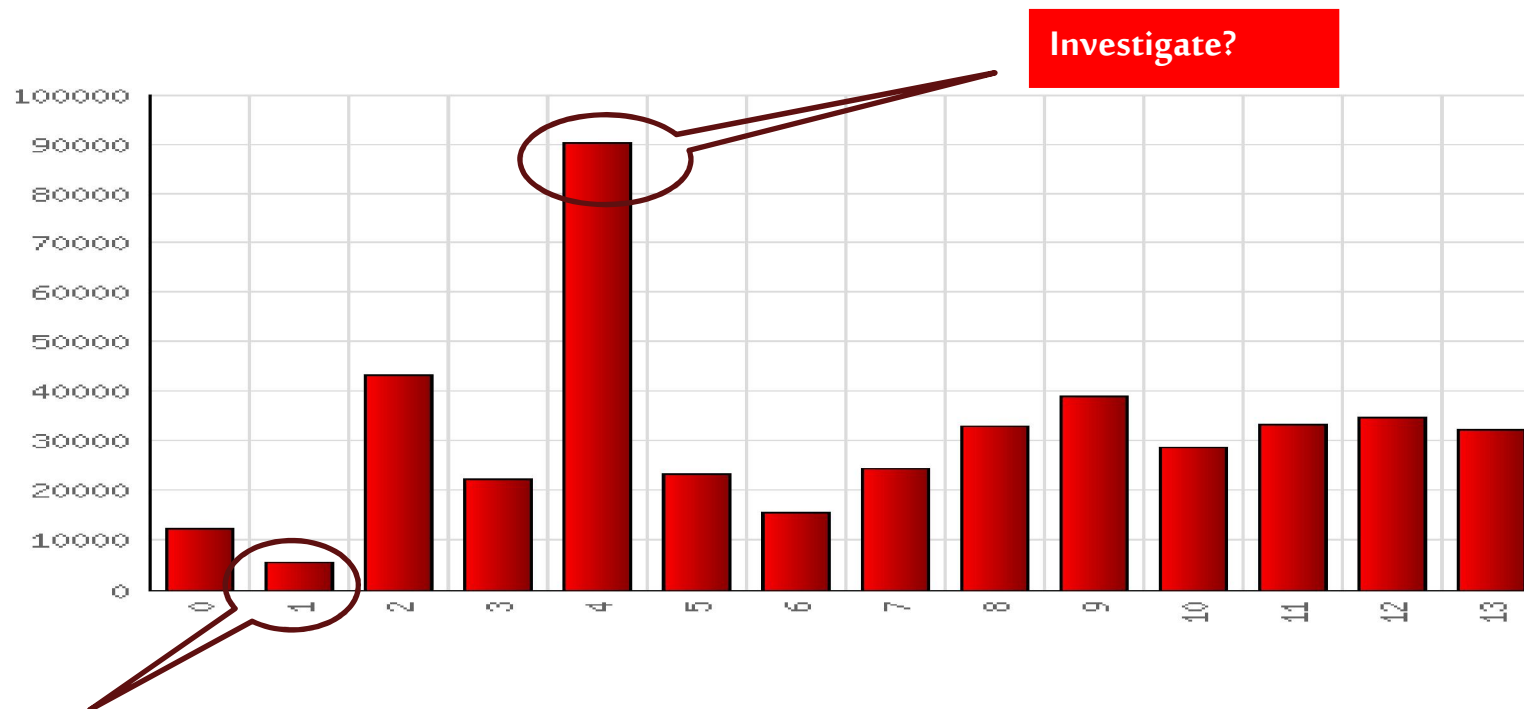
---

- 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.



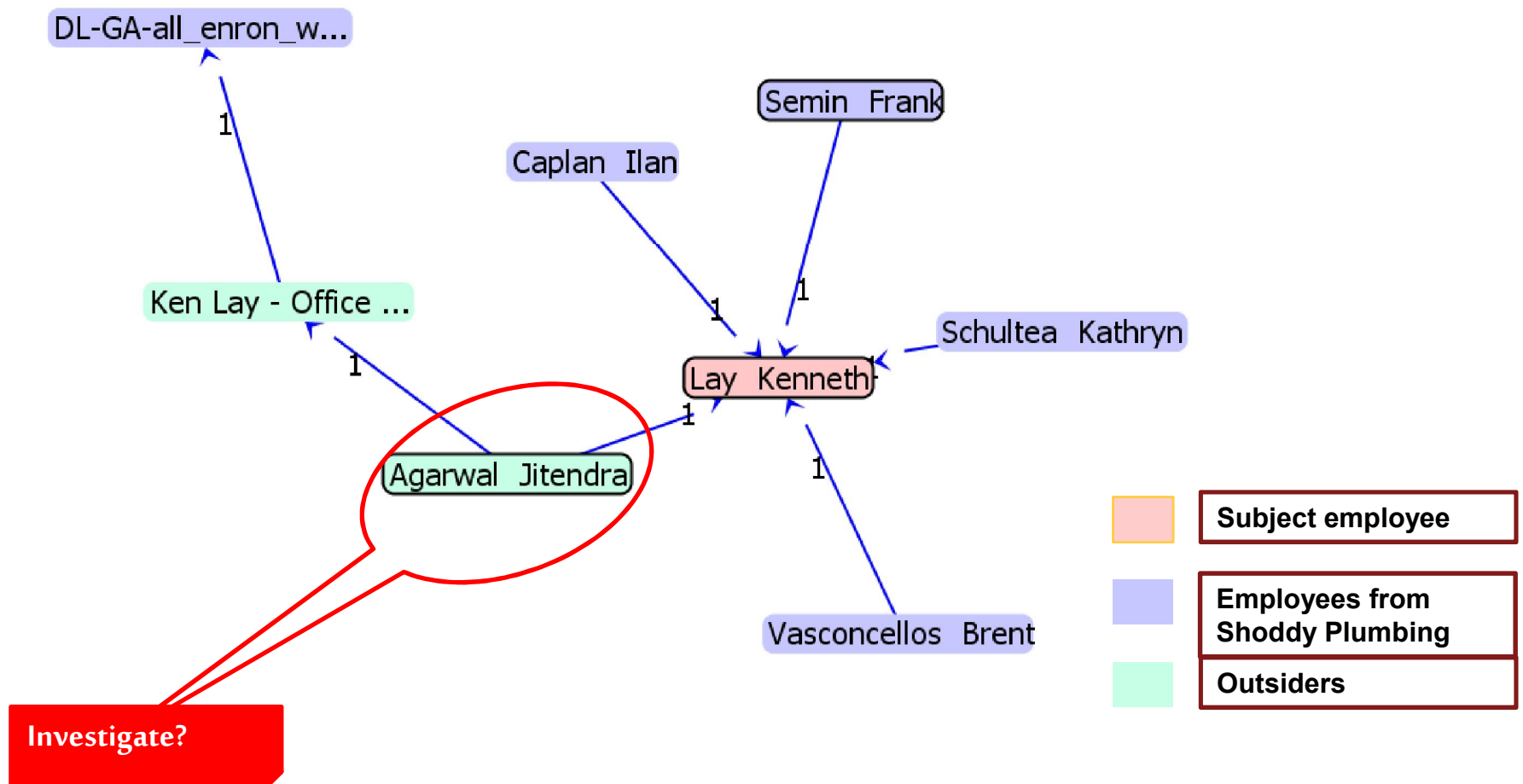
## Sample results of proactive data analytics

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



Ignore?

## Sample results of relationship mapping



## *Do organisations conduct risk assessments?*

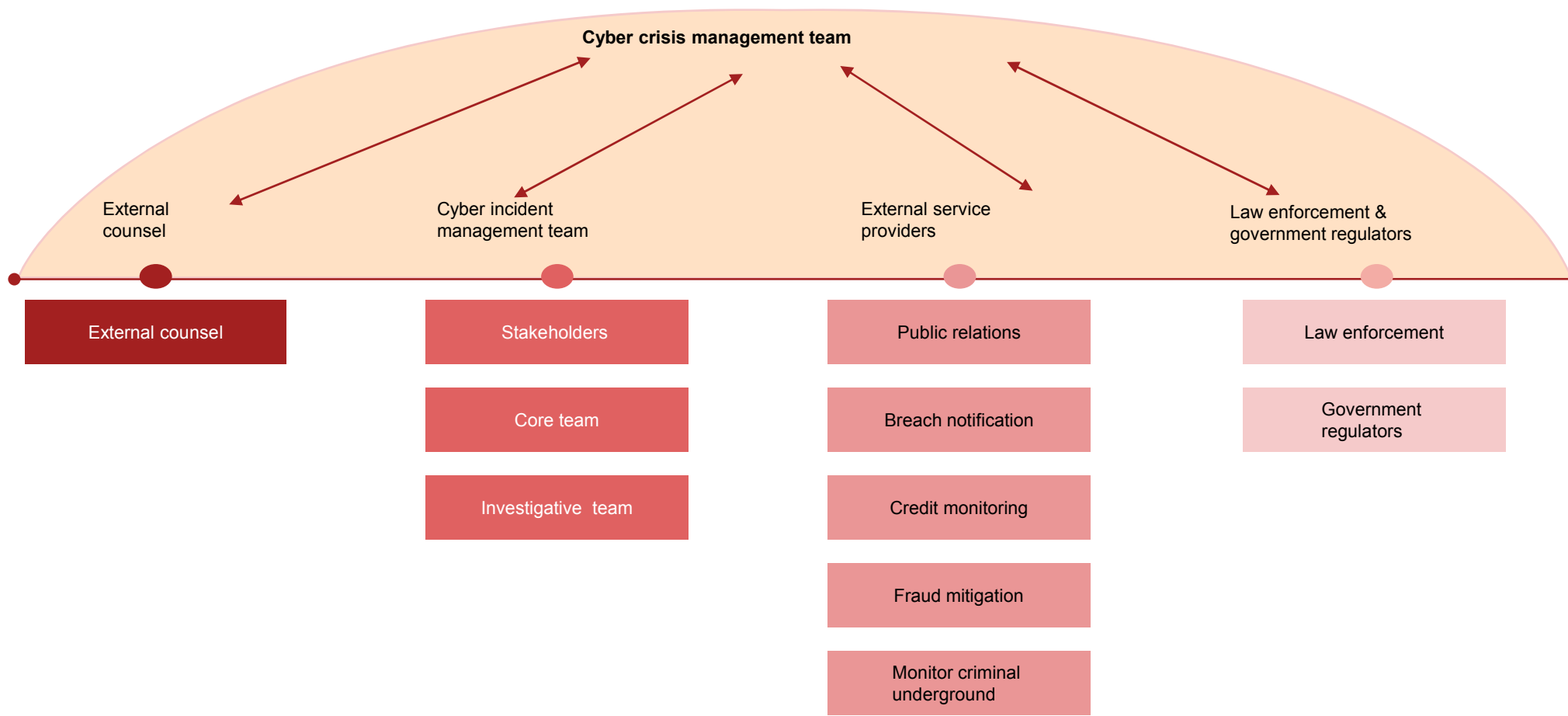
**30%**  
*of Kenya respondents  
have an incident  
response plan*

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.

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

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*



## *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)*

