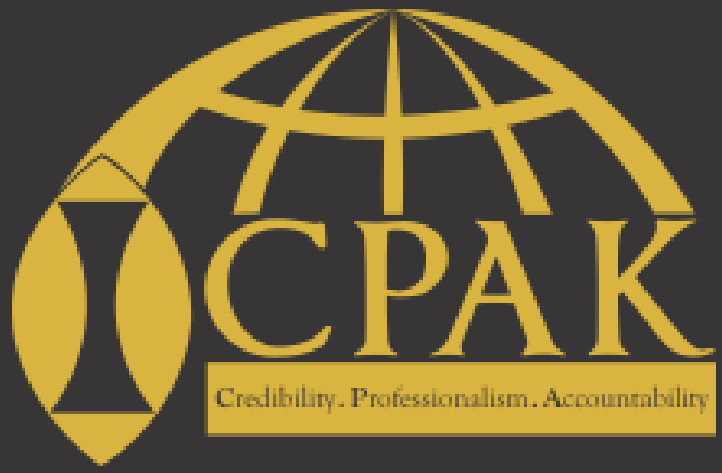


Nasumba Kizito Kwatukha

CPA,CIA,CISA,CISM,CFE,CRMA,CISSP


LOTTERY
WINNER

Content

- **Topic 1: Introduction to Fraud and Technology**

- **Topic 2: Emerging Critical Technology Threats & Attacks**

- **Topic 3: Practical Approach to Resilience**

- **Topic 4: General Data Protection Guidelines**

- **Topic 5: Conclusion/Q&A**

Introduction

- **Fraud is an illegal gain.**
- **Intentional**
- **Secretive – Mostly comes to the fore through a tip off.**

Introduction

- **Consider a long time employee who is suddenly struggling with making ends meet at home.**

- **Through many years of service in the procurement department, he has gained the trust of coworkers, established personal relationships with vendors, and has an intimate knowledge of the controls system and any gaps that may exist.**

- **Almost effortlessly, he could approach a vendor to inflate invoices and direct surplus payments to his personal bank account.**

- **Such collusion is common in procurement frauds.**

Introduction

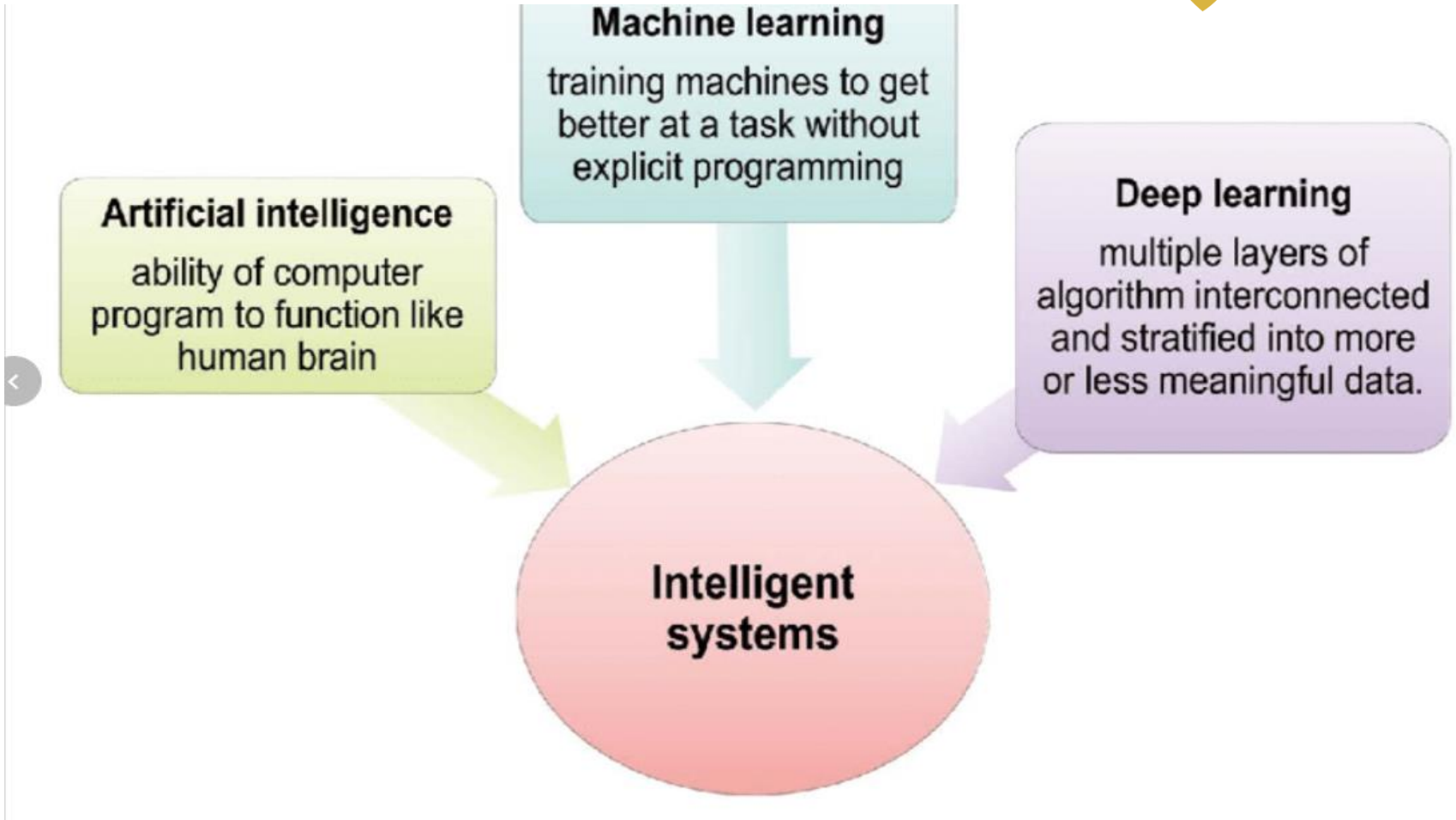
Introduction

- **Technology fraud:**

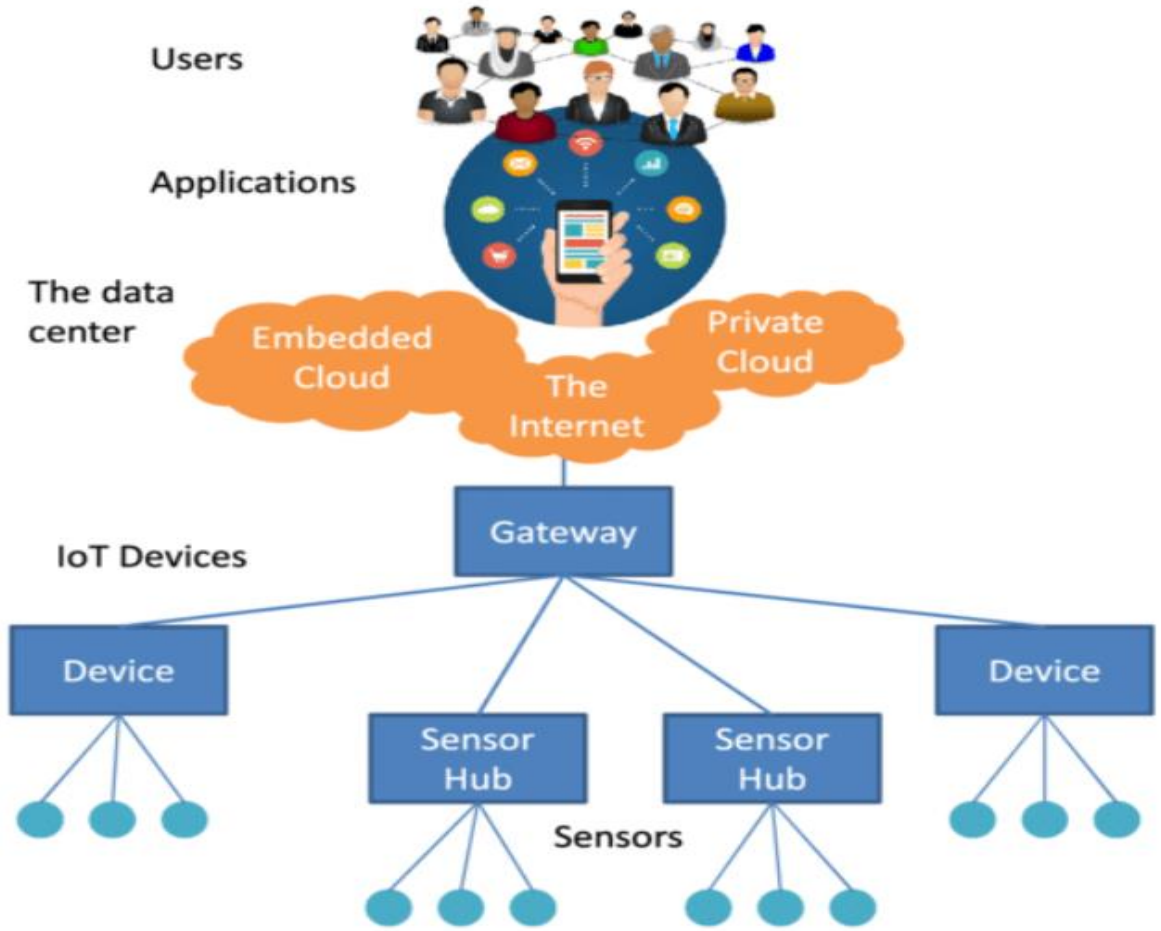
- **Intentional. Happens through the system or with the aid of the system.**

- **Purely technology driven.**

Technology – Intelligent Systems



Internet of things- I.o.T



Technology Universe

- **Technology consists of the following:**
  - **Networks**
  - **Databases**
  - **Email and Biometric**
  - **Computers and Cloud systems**
  - **Mobile phones and Accessories- Recordings**

Technology Universe

Evidence structure in technological spaces still remain as the evidence structure in structured areas namely:

-Relevance

-Reliability

-Sufficiency

-Trace of Evidence: Excel worksheets; Rebooting of machines.

Table of Content

Example of a threat

1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

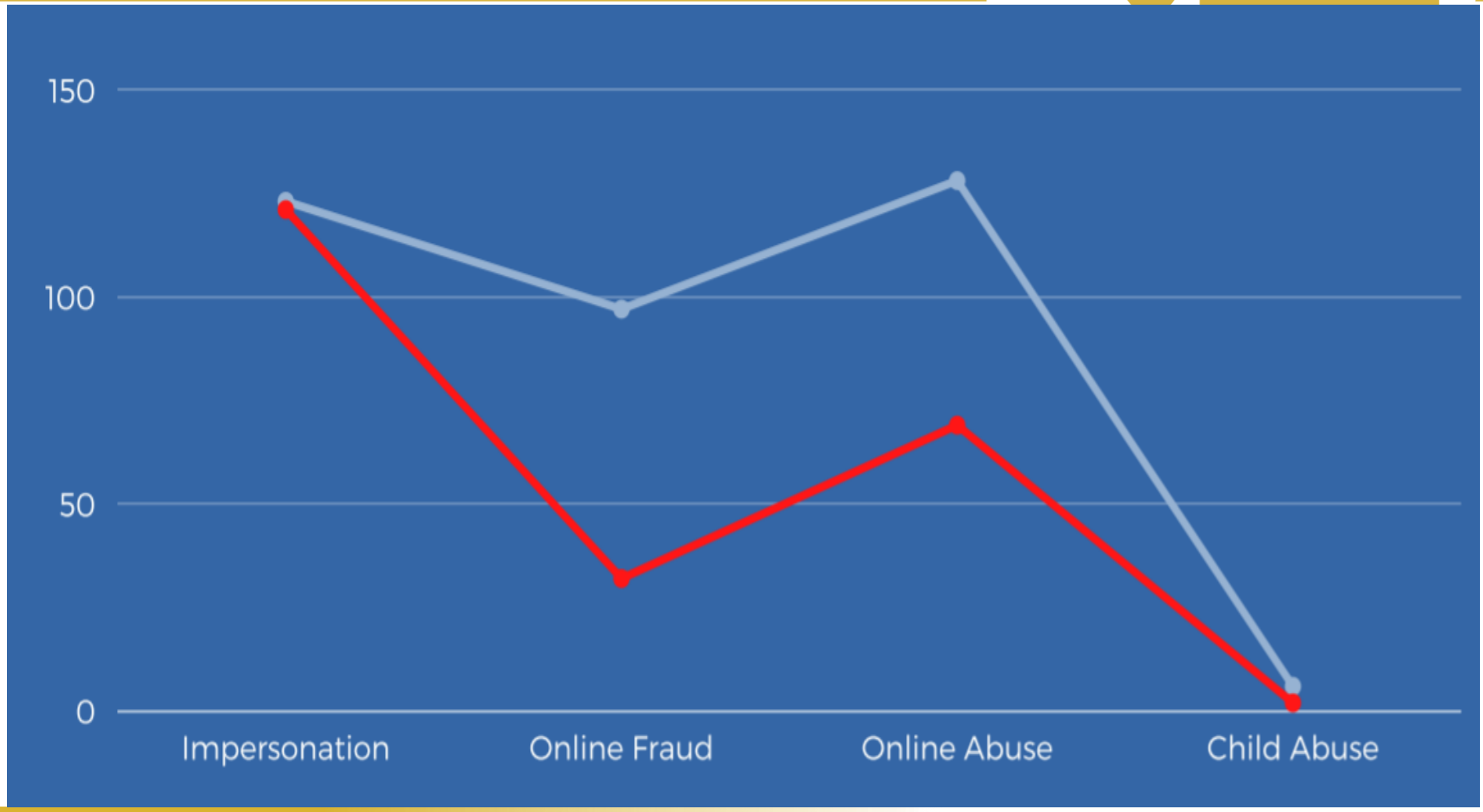
5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Statistics of Tech. Fraud trends in Kenya

46,069,525	The number of malware threat events detected during the period October - December 2020.
2,260,036	The number of DDoS/Botnet threat events detected during the period October - December 2020.
7,847,457	The number of Web Application attack threat events detected during the period October - December 2020.
29,079	The number of System Vulnerabilities threat events detected during the period October - December 2020.

Statistics of Threat Types in Kenya



Technological Fraud trends in Kenya

Areas largely exploited by Fraudsters

- **-Impersonation : Key Loggers**
- **-Malware Attacks**
- **-Phishing**
- **-System Vulnerabilities**
- **-Web Based Attacks**
- **-BOTNET/ DDOS**

Impersonation

https://www.standardmedia.co.ke › Counties › Nairobi

How men mimicked Uhuru to con Naushad Merali Sh10m

26 Feb 2019 — A city tycoon lost Sh10 million to men who **mimicked** President **Uhuru Kenyatta in** a purported land transaction, a court was told on Monday.

https://twitter.com › status

K24 TV on Twitter: "7 suspects who allegedly conned Sameer ...

7 suspects who allegedly **conned** Sameer Africa Chairman Naushad **Merali** 10M **by mimicking** president **Uhuru Kenyatta's voice** arraigned.

Impersonation

https://jalangotv.com › Updates

Martha Karua Among Kenyans Conned Ksh800K By Shirleen ...

17 Nov 2021 — According to popular blogger **Edgar Obare**, **the woman** identified as ... According to the source, part of the **money raised** was intended to ...

https://www.bbc.com › news › world-africa-44899854

Phone scam: How Kenyans are losing money - BBC News

20 Jul 2018 — Mobile phones in **Kenya** are like bank accounts - and fraudsters are trying to hack them.

https://www.bbc.com › news › world-africa-57255600

Letter from Africa: The lure of the get-rich-quick scam in Kenya

1 Jun 2021 — In one of the cryptocurrency scams investors, mostly **Kenyans**, are said to have lost more than $25m, and have not recovered their **money**. I spoke ...

Impersonation

Wangiri, a Japanese word meaning 'one telephone ring and cut,' sees criminals defrauding unwitting victims when they return a missed international call. The call is charged to the victim at a high cost, with the scammers claiming the fee.

Unlike other frauds such as the business email compromise, Wangiri uses uncomplicated technology and may target anyone with a SIM card connection. The fraud **exploits people's innate curiosity to follow up on a missed international call or to respond to a text message.** The country of origin of the call may vary, but could also tally with where the victim has a relative, applied for a job, or visited before.

Once the victim returns the call, the criminals use tactics to keep them on the line for as long as possible to incur higher charges. Some callers are put on hold, spoken to in a foreign langua , tery or that they are being head-hunted for a job interview.

Malware

- **Refers to any malicious code or program such as viruses, bugs, worms, bots, rootkits, spyware, adware, Trojans, and even ransomware that gives a cybercriminal explicit control over your system.**

  - **Information stealers-** Scanning and password crackers of networks
  - **email harvesters-** Loading email with incorrect password; prompt alerts***(Number 7 will shock you)***
  - **Weak authentication- Learning pattern based on Application intelligence and cultural orientation**

  - **ransomware to devices and systems**

Malware

- **This involves a fraudulent attempt by a cybercriminal to obtain sensitive data by posing as a trustworthy party. Spam is the unsolicited sharing of messages with the intention of broadcasting unwanted or malicious content.**

- **M.D@Madison.co.ke and MD@Madison.co.ke**

- **Domain Spoofing : Two unauthentic and Authentic websites**
- **Prices of products e.g a campaigns on products on offer**

Malware


GILBEY'S
GIN
SAVE 331/-
WAS 1,200/-
NOW
869 00
750ML
GILBEY'S GIN
narvas

Web Application Attacks

Web Application attacks are executed by leveraging on web application vulnerabilities such as:

- **Misconfiguration in websites application code, that allow cyber criminals to gain control of the website.**
- **Adoption of unsecured online platforms,**
- **Failure to updated plugins, and lack of technical capacity to secure these platforms amongst users.**

Notable web application attacks will include

- **Code injection attacks to WordPress sites this vulnerability in the plugin allows cyber criminals to install payment skimmers, to crash the site, or retrieve information via SQL injection through brutal force**

Denial of Service(DOS)

- **Denial of Service(DOS) is the worst as it leaves the organization vulnerable without service.**

- **Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding IT infrastructure with a flood of Internet traffic.**

- **A botnet is a group of Internet connected devices running automated tasks over the Internet and which can be used to perform DDoS attacks.**

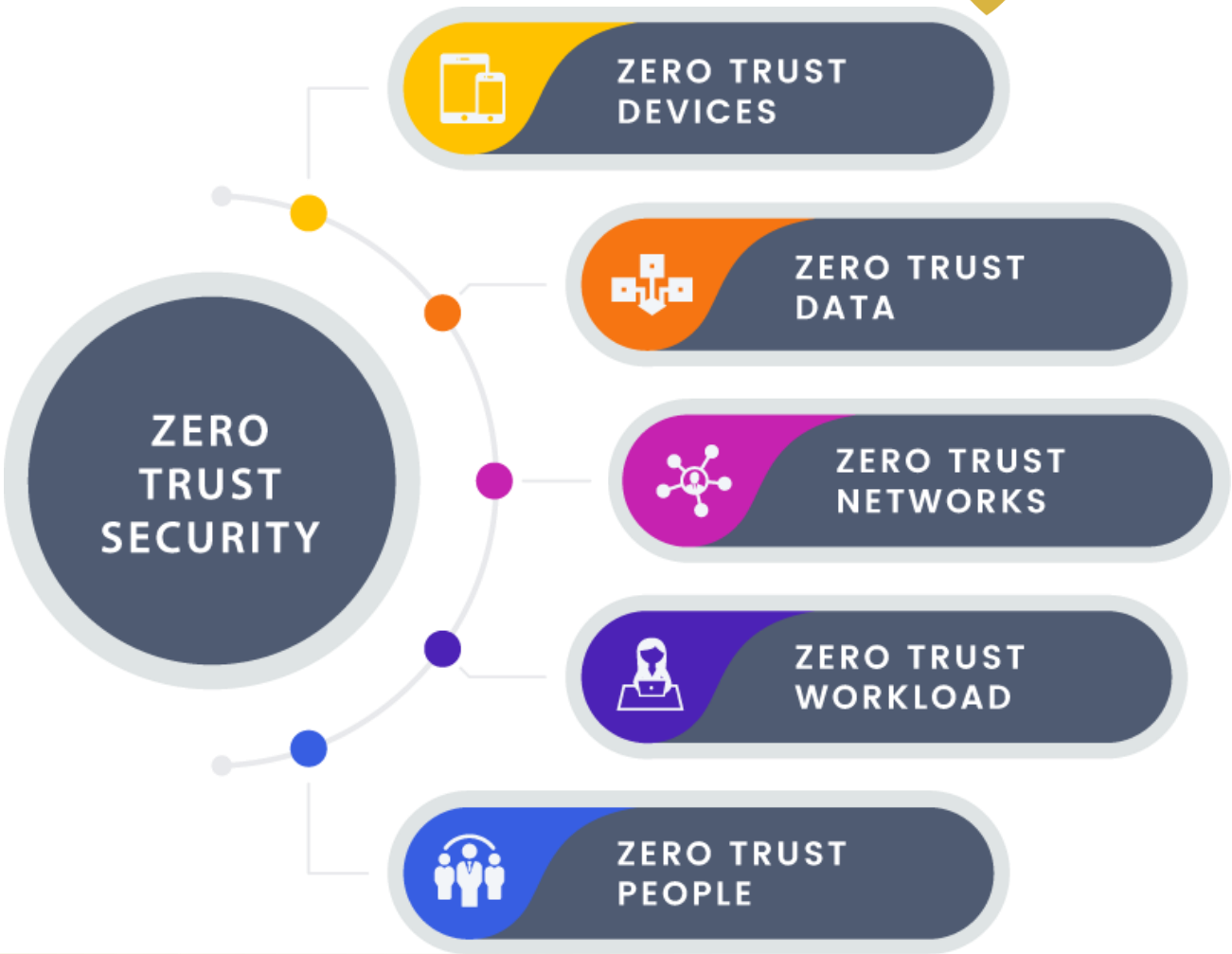
Resilience and Technologies

- Topic 1: Introduction to Fraud and Technology
- Topic 2: Emerging Critical Technology Threats & Attacks
- Topic 3: Practical Approach to Resilience
- Topic 4: Technology Fraud Best Practices
- General Data Protection Guidelines
- Topic 5: Conclusion/Q&A

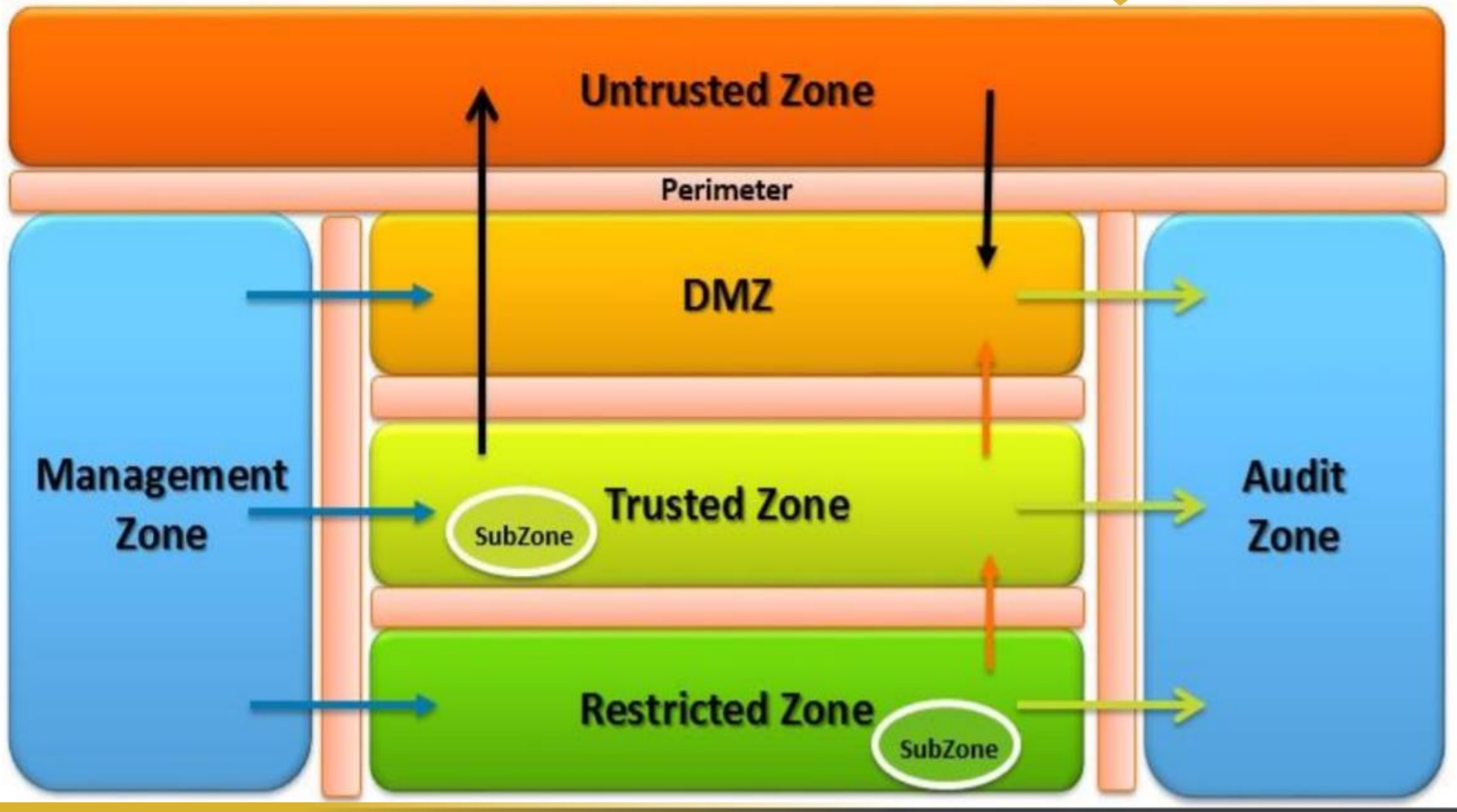
Resilience and Technologies Traditional Approach

- Annual audits (Checklists)
- Annual Pentest and Vulnerability tests
- Authentication mechanisms and Anti viruses(two factor levels is encouraged)
- Certifications

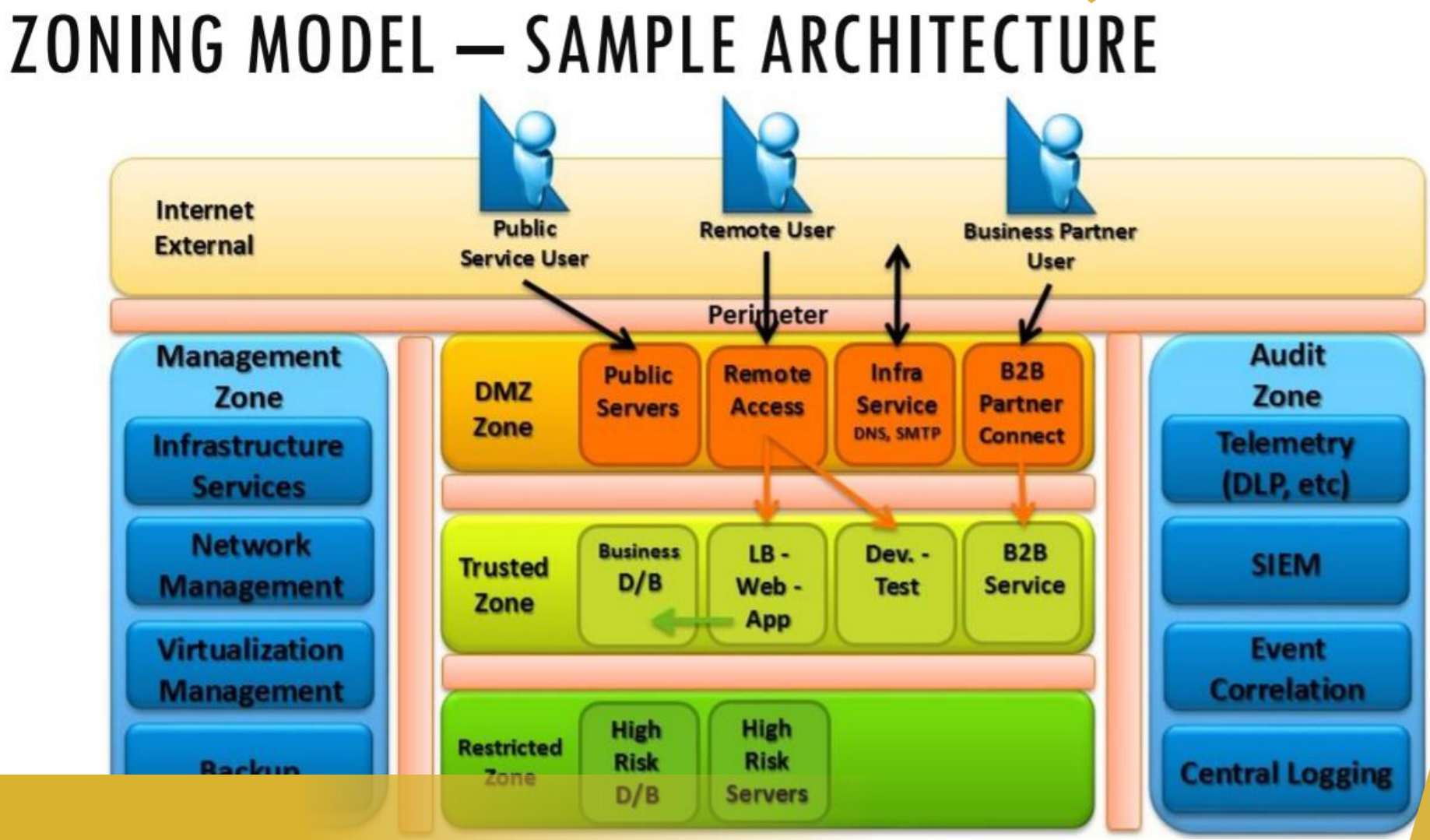
Resilience and Technologies



Resilience and Technologies



Resilience and Technologies



CPAK
Credibility. Professionalism. Accountability

Resilience and Technologies

1. **Email Security**
   - ❑ **DMARC:** Domain-based Message Authentication, Reporting and Conformance
2. **Endpoint Security (User Machines)**
   - ❑ Antivirus
3. **Network Security**
   - ❑ SIEM |SOAR | NAC
4. **Access Management**
   - ❑ NAC
   - ❑ Firewall
5. **Change Management**
   - ❑ FIM (File Integrity Manager)

Content

- Topic 1: Introduction to Fraud and Technology
- Topic 2: Emerging Critical Technology Threats & Attacks
- Topic 3: Practical Approach to Resilience
- Topic 4: General Data Protection Guidelines
- Topic 5: Conclusion/Q&A

General Data Protection Guidelines

- These regulations set out the procedures for enforcement of the rights of the data subjects as well as elaborating on the duties and obligations of Data Controllers and Data Processors.

- **Data Commissioner:** *This means a natural or legal person, public authority, agency, or other body which alone, or jointly with others, determines the purpose and means of processing of personal data.*
- **Data *Processor: This*** *means a natural or legal person, public authority, agency, or other body which alone or jointly with others processes personal data on behalf of the data controller.*

General Data Protection Guidelines

- **Personal data:** this means any information relating to an identified or identifiable natural person. Includes a person's full name, identity card number, date of birth, gender, physical and postal address.

- **Sensitive data: means** sensitive personal data means data revealing a person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of a person's children, parents, spouse or spouses, sex, or sexual orientation.

- **Pseudonymisation:** This is defined as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin,

General Data Protection Guidelines

- Consent of the Data Subject
- Collection of Personal Data
- Enabling the rights and processing of data
- Commercial Use and objection to use of Personal Data
- Obligations of Data controllers and Data Processors
- Data Protection by Design or Default
- Notification of Personal Data Breaches
- Transfer of Personal Data Outside Kenya

General Data Protection Guidelines

In obtaining the consent, the data controller and the data processor shall ensure that the data subject:

-Has capacity to understand and communicate.

-Is informed of the nature of processing in simple and clear language that is understandable.

-Voluntarily gives consent

-Consent is specific Consent may be oral, in writing or electronic.

This includes data shared during interviews and CVs and information captured during investigation

General Data Protection Guidelines

Collection of personal data entails obtaining personal data directly from the data subject or by any means including from—

- Any other person
- Generally available publications or databases
- Surveillance cameras, where an individual is identifiable or reasonably identifiable
- Information associated with web browsing, including information collected by cookies
- Biometric technologies.

General Data Protection Guidelines

Data Controllers and Processors shall have regard to the following during data collection:

- Collecting what one is permitted to under the law.
- Ensure data quality and accuracy
- Secure the personal data collected
- Only collect sensitive personal data from the data subject

General Data Protection Guidelines

Rights of Data Subjects

- Right to access personal data
- Right to restrict processing
- Right to object to processing
- Right of rectification
- Data portability request
- Right of erasure

General Data Protection Guidelines

Obligations of Data controllers and Data Processors:

- Limitation on the retention of personal data
- Requests to anonymize or Pseudo personal data
- Sharing of personal data
- Automated individual decision making
- Data protection Policy Agreements between data controllers and data processors Engagement of a third party in the processing activities.

General Data Protection Guidelines

- Requirements prior to transfer:
- Legally enforceable obligations;
- Consent to transfer from data subject.
- Cross Boarder transfer Agreements
- Legally enforceable obligations

Any country or a territory is taken to have appropriate safeguards for purposes of section 49(1) if the country or territory has:

- Ratified the African Union Convention on Cyber Security and Personal Data Protection;
- Reciprocal data protection agreement with Kenya
- An adequate data protection law as shall be determined by the Data Commissioner.

General Data Protection Guidelines

Exemptions to Data Laws

– National Security

– Public Interest

– Permitted General Situation

– Permitted Health Situation

ICPAK
Credibility. Professionalism. Accountability