COURSE FACILITATOR

CHRISPUS ALUKWE AKHONYA – CEH|MSc|BSc|CSCU:

alukchris@gmail.com
+254720474923 | +254780474923
caakhonya@usiu.ac.ke

Introduction

COMPUTER FRAUD AND ABUSE

Introduction

- Companies face four types of threats to their information systems:
  - Natural and political disasters
  - Software errors and equipment malfunction
  - Unintentional acts
  - Intentional acts (including computer crime)

Fraud Defined

- ***Fraud*** is any and all means a person uses to gain an unfair advantage over another person.
- Typically, a fraudulent act must involve:
  - A false statement
  - A material fact
  - Knowledge
  - Reliance
  - Injury or loss

Fraud Defined

- Three types of fraud:
  - Misappropriation of assets
  - Corruption
  - Fraudulent statements

Treadway Commission

- The National Commission on Fraudulent Financial Reporting (*aka*, the Treadway Commission) defined ***fraudulent financial reporting*** as intentional or reckless conduct, whether by act or omission, that results in materially misleading financial statements.

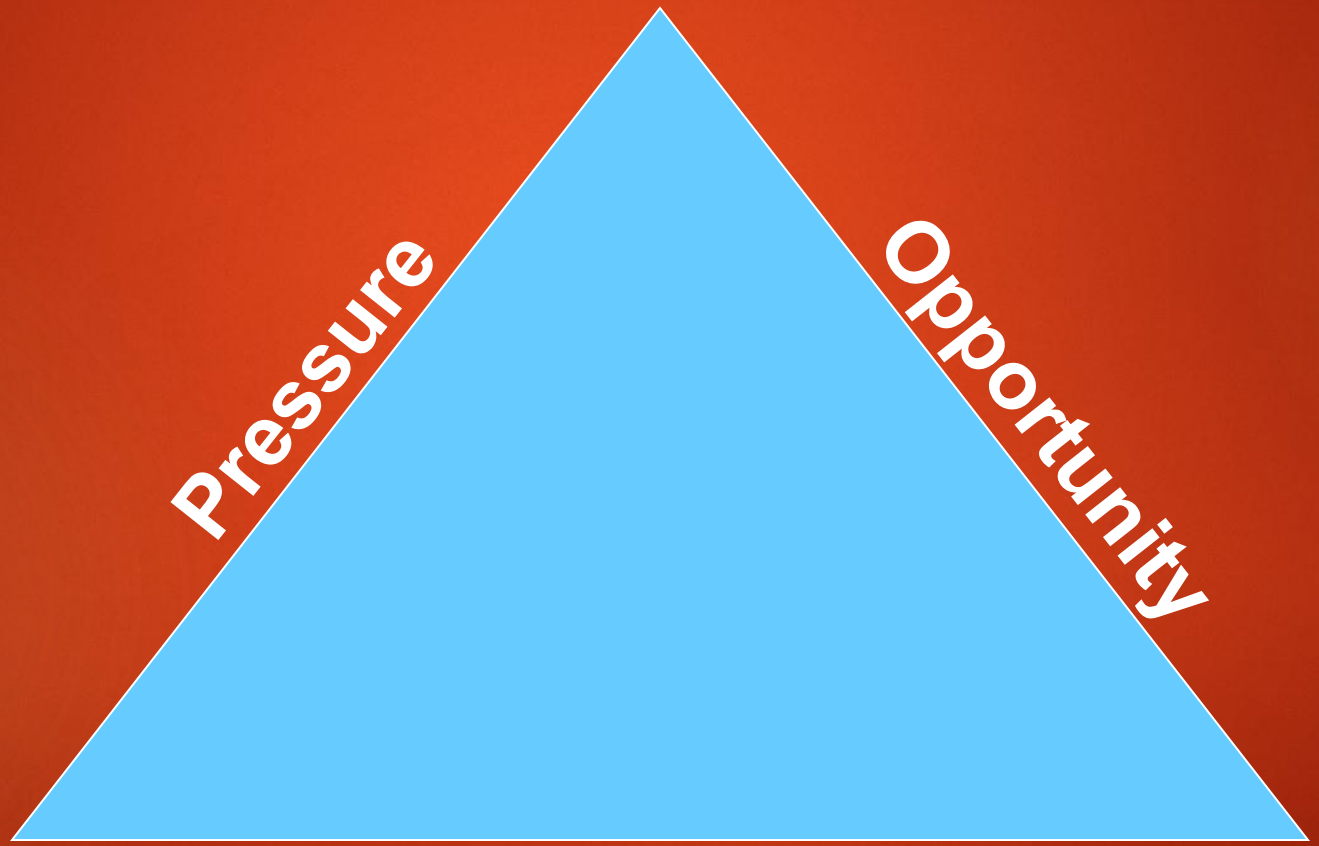
SAS-99 *(Is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) in October 2002)*

- The Auditor's Responsibility to Detect Fraud requires auditors to:
  - Understand fraud
  - Discuss the risks of material fraudulent misstatements
  - Obtain information
  - Identify, assess, and respond to risks
  - Evaluate the results of their audit tests
  - Communicate findings
  - Document their audit work
  - Incorporate a technology focus

Who Commits Fraud and Why

- White collar criminals
- Violent criminals
- Hackers
- Computer fraud perpetrators

The Fraud Triangle



Rationalization

Action of attempting to explain or justify behaviour or an attitude with logical reasons, even if these are not appropriate

The Fraud Triangle: Pressures

- The most common pressures were:
  - Financial
    - Not being able to pay one's debts, nor admit it to one's employer, family, or friends
    - Business reversals
  - Emotional
    - Fear of loss of status
    - Physical isolation
    - Difficulties in employer-employee relations
  - Lifestyle
    - Status gaining
    - Drug/alcohol addiction
    - Gambling

The Fraud Triangle: Pressures

- Common pressures in financial statement fraud include the need to:
  - Prop up earnings or stock price OR to reduce earnings
  - Cover the inability to generate cash flow
  - Obtain financing
  - Appear to comply with bond covenants or other agreements

The Fraud Triangle: Opportunity

- Opportunity is the opening or gateway that allows an individual to:
  - Commit the fraud
  - Conceal the fraud
    - Expensing
    - Lapping
    - Kiting
  - Convert the proceeds

The Fraud Triangle: Opportunity

- Common opportunities that enable fraud:
  - Lack of internal controls
  - Failure to enforce controls
  - Excessive trust in key employees
  - Incompetent supervisory personnel
  - Inattention to details
  - Inadequate staff

The Fraud Triangle: Opportunity

- Internal controls that may be lacking or un-enforced include:
  - Authorization procedures
  - Clear lines of authority
  - Adequate supervision
  - Adequate documents and records
  - A system to safeguard assets
  - Independent checks on performance
  - Separation of duties

The Fraud Triangle: Opportunity

- Management may allow fraud by:
  - Not getting involved in the design or enforcement of internal controls;
  - Inattention or carelessness;
  - Overriding controls; and/or
  - Using their power to compel subordinates to carry out the fraud.

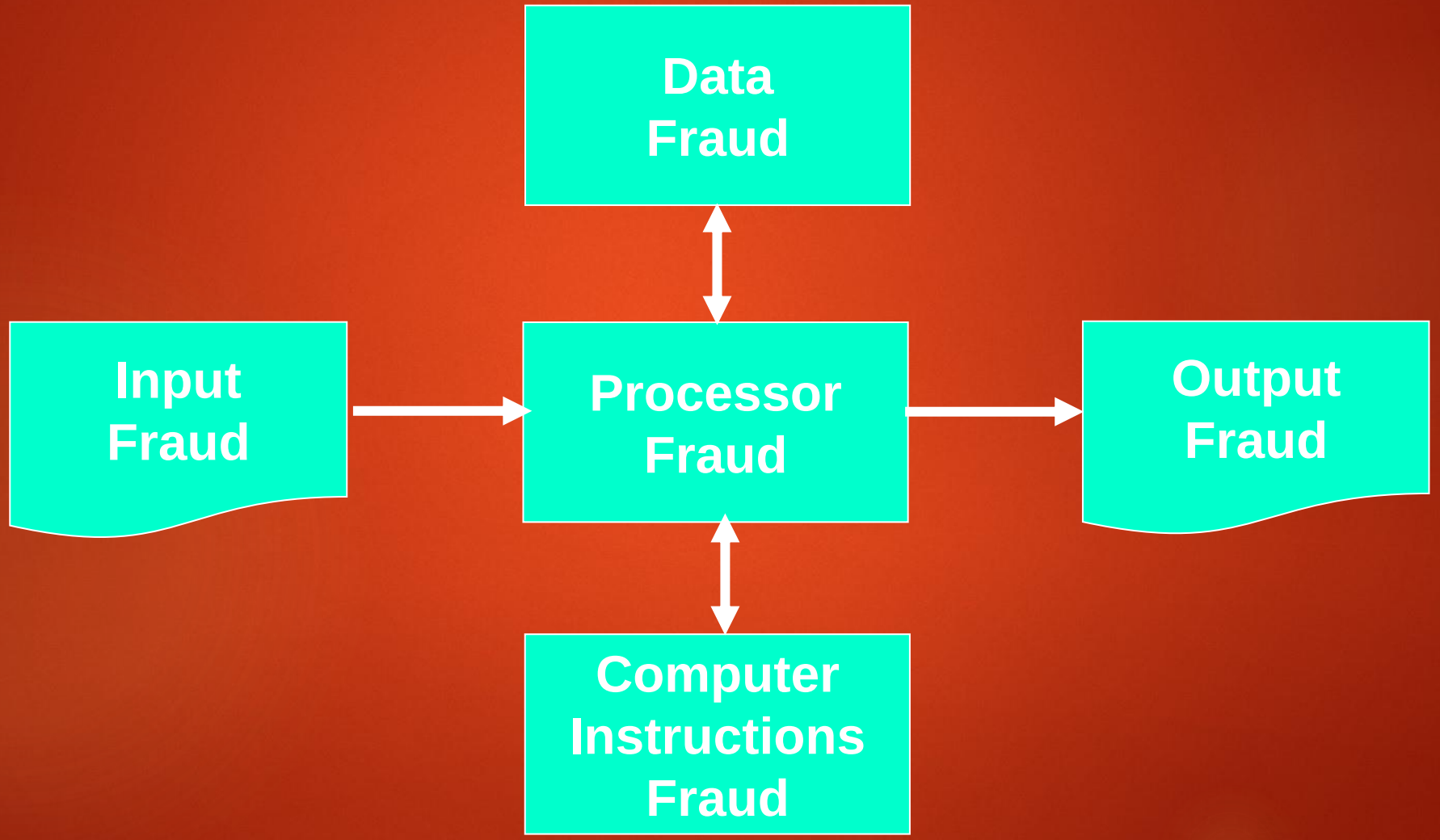
The Fraud Triangle: Summary

- Fraud occurs when:
  - People have perceived, non-shareable ***pressures***;
  - The ***opportunity*** gateway is left open; and
  - They can ***rationalize*** their actions to reduce the moral impact in their minds (i.e., they have low integrity).
- Fraud is much less likely to occur when
  - There is low pressure, low opportunity, and high integrity.

Computer Fraud

- Any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution
- What are examples of computer fraud?
  - unauthorized use, access, modification, copying, and destruction of software or data
  - theft of money by altering computer records or the theft of computer time
  - theft or destruction of computer hardware
  - use or the conspiracy to use computer resources to commit a felony
  - intent to illegally obtain information or tangible property through the use of computers

Computer Fraud: Classifications



Computer Fraud: Classifications

- ***Processor Fraud***
  - Involves unauthorized system use
  - Includes theft of computer time and services.

Computer Fraud: Classifications

- ***Computer Instructions Fraud***
  - Involves tampering with software that processes company data
  - May include:
    - Modifying the software
    - Making illegal copies
    - Using it in an unauthorized manner

Computer Fraud: Classifications

- ***Data Fraud***
  - Involves:
    - Altering or damaging a company's data files; or
    - Copying, using, or searching the data files without authorization.
  - Sale of stolen data

Computer Fraud: Classifications

- ***Output Fraud***
  - Stealing or misusing system output.
  - Use computers and peripheral devices to create counterfeit outputs

Computer Fraud and Abuse Techniques

- Data diddling
- Data leakage
- Denial of service attacks
- Eavesdropping
- Email threats
- Email forgery
- Hacking
- Phreaking
- Hijacking
- Identity theft

Computer Fraud and Abuse Techniques

- Internet misinformation
- Internet terrorism
- Logic time bombs
- Masquerading or impersonation
- Packet sniffers
- Password cracking
- Phishing
- Piggybacking
- Round-down technique
- Salami technique

Computer Fraud and Abuse Techniques

- Social engineering
- Software piracy
- Spamming
- Spyware
- Keystroke loggers
- Superzapping
- Trap doors
- Trojan horse
- War dialing
- War driving

Computer Fraud and Abuse Techniques

- Virus
- Worms
- The low-tech, do-it-yourself attack

Deterring and Detecting Computer Fraud

- Measures to decrease the potential for fraud and resulting losses:
  - Make fraud less likely to occur
  - Increase the difficulty of committing fraud
  - Improve detection methods
  - Reduce fraud losses

Deterring and Detecting Computer Fraud

- ***Make fraud less likely to occur***
  - Culture that stresses integrity
  - Organizational structure, management philosophy, and operating style
  - Independent audit committee
  - Assign authority and responsibility
  - Identify risky areas
  - Develop a comprehensive set of security policies
  - Implement human resource policies that send messages about ethical behavior and integrity
  - Effectively supervise employees

Deterring and Detecting Computer Fraud

- Train employees in integrity and ethical considerations, as well as security and fraud prevention measures.
- Require annual employee vacations and periodic rotation of duties
- Implement project development and acquisition controls
- Prosecute fraud perpetrators more vigorously

Deterring and Detecting Computer Fraud

- ***Increase the difficulty of committing fraud***
  - Develop a strong system of internal controls
  - Segregate the accounting functions of:
    - Authorization
    - Recording
    - Custody
  - Implement segregation of duties between systems functions
  - Restrict physical and remote access to system resources

Deterring and Detecting Computer Fraud

- Require authorization of transactions and activities
- Adequate design of documents and records
- Safeguard all assets, records, and data
- Require independent checks
- Implement computer-based controls
- Encryption of stored and transmitted data
- Install latest updates to software

Deterring and Detecting Computer Fraud

- ***Improve detection methods***
  - Create an audit trail
  - Conduct periodic audits
  - Install fraud detection software
  - Implement a fraud hotline
  - Employ a computer security officer
  - Monitor system activities
  - Use intrusion detection systems

Deterring and Detecting Computer Fraud

- ***Reduce Fraud Losses***
  - Maintain adequate insurance
  - Develop comprehensive fraud contingency, disaster recovery, and business continuity plans
  - Backup copies
  - Monitor system activity

Summary

- We have:
  - Defined fraud
  - Described the Fraud Triangle (the fraud process)
  - Discussed who perpetrates a fraud and why they do it, including:
    - Pressures
    - Opportunities
    - Rationalizations
  - Defined computer fraud
  - Discussed computer fraud classifications
  - Compared and contrasted the approaches and techniques used to commit computer fraud

Q & A

CEH-Alukwe - 0720474923 | 0780474923
cakhonya@kabarak.ac.ke | alukchris@gmail.Com