CHAPTER 5

COMPUTER FRAUD AND SECURITY
Overview

• Information systems are becoming increasingly more complex and society is becoming increasingly more dependent on these systems.
  – Companies also face a growing risk of these systems being compromised.
  – Recent surveys indicate 67% of companies suffered a security breach in the last year with almost 60% reporting financial losses.
The information security system is the subsystem of the organization that controls the special risks associated with computer-based information systems.

The information security system has the basic elements of any information system, such as hardware, databases, procedures, and reports.
Companies face four types of threats to their information systems:

1- Natural and political disasters

- Include: Fire or excessive heat, Floods, Earthquakes, High winds, War and terrorist attack

- When a natural or political disaster strikes, many companies can be affected at the same time.
  - Example: Bombing of the World Trade Center in NYC.

- The Defense Science Board has predicted that attacks on information systems by foreign countries, espionage agents, and terrorists will soon be widespread.
Overview

2- Software errors and equipment malfunction

- Include:
  - Hardware or software failures
  - Software errors or bugs
  - Operating system crashes
  - Power outages and fluctuations
  - Undetected data transmission errors

- Estimated annual economic losses due to software bugs = $60 billion.
- 60% of companies studied had significant software errors in previous year.
Overview

3- Unintentional acts

- Include
  - Accidents caused by:
    - Human carelessness
    - Failure to follow established procedures
    - Poorly trained or supervised personnel
  - Innocent errors or omissions
  - Lost, destroyed, or misplaced data
  - Logic errors
  - Systems that do not meet needs or are incapable of performing intended tasks
- Information Systems Security Assn. estimates 65% of security problems are caused by human error.
4- **Intentional acts (computer crime)**

- Include:
  - Sabotage
  - Computer fraud
  - Misrepresentation, false use, or unauthorized disclosure of data
  - Misappropriation of assets
  - Financial statement fraud
- Information systems are increasingly vulnerable to these malicious attacks.
The Information Security System in the Organization

The information security system must be managed by a chief security officer (CSO).

This individual should report directly to the board of directors in order to maintain complete independence.
The Fraud Process

• **Fraud** is any and all means a person uses to gain an unfair advantage over another person.

• In most cases, to be considered fraudulent, an act must involve:
  – A false statement (oral or in writing)
  – About a material fact
  – Knowledge that the statement was false when it was uttered (which implies an intent to deceive)
  – A victim relies on the statement
  – And suffers injury or loss as a result
The Fraud Process

• Since fraudsters don’t make journal entries to record their frauds, we can only estimate the amount of losses caused by fraudulent acts:
  – The Association of Certified Fraud Examiners (ACFE) estimates that total fraud losses in the U.S. run around 6% of annual revenues or approximately $660 billion in 2004.
    • More than we spend on education and roads in a year.
    • 6 times what we pay for the criminal justice system.
  – Income tax fraud (the difference between what taxpayers owe and what they pay to the government) is estimated to be over $200 billion per year.
  – Fraud in the healthcare industry is estimated to exceed $100 billion a year.
The Fraud Process

• Fraud against companies may be committed by an employee or an external party.
  – Former and current employees (called knowledgeable insiders) are much more likely than non-employees to perpetrate frauds (and big ones) against companies.
    • Largely owing to their understanding of the company’s systems and its weaknesses, which enables them to commit the fraud and cover their tracks.
  – Organizations must utilize controls to make it difficult for both insiders and outsiders to steal from the company.
Types of Frauds

**OCCUPATIONAL**
- Fraudulent Statements
  - Financial
  - Non-financial
- Asset Misappropriation
  - Theft of Cash
  - Fraudulent disbursements
  - Inventory and other assets
- Bribery and Corruption
  - Bribery
  - Illegal gratuities
  - Economic extortion
  - Conflict of interest

**OTHER**
- Intellectual property theft
- Financial institution fraud
- Check and credit card fraud
- Insurance fraud
- Healthcare fraud
- Bankruptcy fraud
- Tax fraud
- Securities fraud
- Money laundering
- Consumer fraud
- Computer and Internet fraud
The Fraud Process

• Three types of occupational fraud:

  1- Misappropriation of assets

  • Involves theft, embezzlement, or misuse of company assets for personal gain.
  • Examples include billing schemes, check tampering, skimming, and theft of inventory.
  • In the 2004 Report to the Nation on Occupational Fraud and Abuse, 92.7% of occupational frauds involved asset misappropriation at a median cost of $93,000.
The Fraud Process

2- Corruption

- Corruption involves the wrongful use of a position, contrary to the responsibilities of that position, to procure a benefit.
- Examples include kickback schemes and conflict of interest schemes.
- About 30.1% of occupational frauds include corruption schemes at a median cost of $250,000.
The Fraud Process

3- Fraudulent statements

- Financial statement fraud involves misstating the financial condition of an entity by intentionally misstating amounts or disclosures in order to deceive users.
- Financial statements can be misstated as a result of intentional efforts to deceive or as a result of undetected asset misappropriations that are so large that they cause misstatement.
- About 7.9% of occupational frauds involve fraudulent statements at a median cost of $1 million. (The median pales in comparison to the maximum cost.)
The Fraud Process

• A typical employee fraud has a number of important elements or characteristics:
  – The fraud perpetrator must gain the trust or confidence of the person or company being defrauded in order to commit and conceal the fraud.
  – Instead of using a gun, knife, or physical force, fraudsters use weapons of deceit and misinformation.
  – Frauds tend to start as the result of a perceived need on the part of the employee and then escalate from need to greed. Most fraudsters can’t stop once they get started, and their frauds grow in size.
  – The fraudsters often grow careless or overconfident over time.
  – Fraudsters tend to spend what they steal. Very few save it.
  – In time, the sheer magnitude of the frauds may lead to detection.
  – The most significant contributing factor in most employee frauds is the absence of internal controls and/or the failure to enforce existing controls.
The Fraud Process

• Financial statements can be falsified to:
  – Deceive investors and creditors
  – Cause a company’s stock price to rise
  – Meet cash flow needs
  – Hide company losses and problems
The Fraud Process

- Fraudulent financial reporting is of great concern to independent auditors, because undetected frauds lead to half of the lawsuits against auditors.
- In the case of Enron, a financial statement fraud led to the total elimination of Arthur Andersen, a premiere international public accounting firm.
The Fraud Process

• **SAS 99: The Auditor’s Responsibility to Detect Fraud**
  
  – In 1997, SAS-82, *Consideration of Fraud in a Financial Statement Audit*, was issued to clarify the auditor’s responsibility to detect fraud.
The Fraud Process

• A revision to SAS-82, SAS-99, was issued in December 2002. SAS-99 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
Approaches to Computer Fraud

• Computer fraud includes the following:
  – Unauthorized theft, use, access, modification, copying, and destruction of software or data.
  – Theft of money by altering computer records.
  – 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.
Approaches to Computer Fraud

• In using a computer, fraud perpetrators can steal:
  – More of something
  – In less time
  – With less effort

• They may also leave very little evidence, which can make these crimes more difficult to detect.
Approaches to Computer Fraud

• Computer systems are particularly vulnerable to computer crimes for several reasons:
  – Company databases can be huge and access privileges can be difficult to create and enforce. Consequently, individuals can steal, destroy, or alter massive amounts of data in very little time.
  – Organizations often want employees, customers, suppliers, and others to have access to their system from inside the organization and without. This access also creates vulnerability.
  – Computer programs only need to be altered once, and they will operate that way until:
    • *The system is no longer in use; or*
    • *Someone notices.*
Approaches to Computer Fraud

- Modern systems are accessed by PCs, which are inherently more vulnerable to security risks and difficult to control.
  - It is hard to control physical access to each PC.
  - PCs are portable, and if they are stolen, the data and access capabilities go with them.
  - PCs tend to be located in user departments, where one person may perform multiple functions that should be segregated.
  - PC users tend to be more oblivious to security concerns.
Approaches to Computer Fraud

– Computer systems face a number of unique challenges:
  • Reliability (accuracy and completeness)
  • Equipment failure
  • Environmental dependency (power, water damage, fire)
  • Vulnerability to electromagnetic interference and interruption
  • Eavesdropping
  • Misrouting
Approaches to Computer Fraud

• Organizations that track computer fraud estimate that most U.S. businesses have been victimized by at least one incident of computer fraud.
Approaches to Computer Fraud

• These frauds cost billions of dollars each year, and their frequency is increasing because:
  – Not everyone agrees on what constitutes computer fraud.
    • Many don’t believe that taking an unlicensed copy of software is computer fraud. (It is and can result in prosecution.)
    • Some don’t think it’s a crime to browse through someone else’s computer if their intentions aren’t malicious.
Approaches to Computer Fraud

- Many computer frauds go undetected.
- An estimated 80-90% of frauds that are uncovered are not reported because of fear of:
  - Adverse publicity
  - Copycats
  - Loss of customer confidence.
- There are a growing number of competent computer users, and they are aided by easier access to remote computers through the Internet and other data networks.
Approaches to Computer Fraud

- Many networks have a low level of security.
- Instructions on how to perpetrate computer crimes and abuses are readily available on the Internet.
- Law enforcement is unable to keep up with the growing number of frauds.
- The total dollar value of losses is difficult to calculate.
Approaches to Computer Fraud

- **Computer Fraud Classification**
  - Frauds can be categorized according to the data processing model:
    - Input
    - Processor
    - Computer instructions
    - Stored data
    - Output
Approaches to Computer Fraud

• **Input Fraud**
  
  – The simplest and most common way to commit a fraud is to alter computer input.
  
  • Requires little computer skills.
  
  • Perpetrator only need to understand how the system operates
Input Fraud

– Can take a number of forms, including:

1- *Disbursement frauds*

• The perpetrator causes a company to:
  – Pay too much for ordered goods; or
  – Pay for goods never ordered.

2- *Inventory frauds*

• The perpetrator enters data into the system to show that stolen inventory has been scrapped.
Input Fraud

3- Payroll frauds

• Perpetrators may enter data to:
  – Increase their salaries
  – Create a fictitious employee
  – Retain a terminated employee on the records.
• In the latter two instances, the perpetrator intercepts and cashes the resulting paychecks.
Input Fraud

4- Cash receipt frauds

- The perpetrator hides the theft by falsifying system input.
- EXAMPLE: Cash of $200 is received. The perpetrator records a cash receipt of $150 and pockets the $50 difference.

5- Fictitious refund fraud

- The perpetrator files for an undeserved refund, such as a tax refund.
Processor Fraud

- Involves computer fraud committed through unauthorized system use.
- Includes theft of computer time and services.
- Incidents could involve employees:
  - Surfing the Internet;
  - Using the company computer to conduct personal business; or
  - Using the company computer to conduct a competing business.
Processor Fraud

• In one example, an agriculture college at a major state university was experiencing very sluggish performance from its server.
• Upon investigating, IT personnel discovered that an individual outside the U.S. had effectively hijacked the college’s server to both store some of his/her research data and process it.
• The college eliminated the individual’s data and blocked future access to the system.
• The individual subsequently contacted college personnel to protest the destruction of the data.
Computer Instructions Fraud

– Involves tampering with the software that processes company data.

– May include:
  • Modifying the software
  • Making illegal copies
  • Using it in an unauthorized manner

– Also might include developing a software program or module to carry out an unauthorized activity.
Computer Instructions Fraud

- Computer instruction fraud used to be one of the least common types of frauds because it required specialized knowledge about computer programming beyond the scope of most users.
- Today these frauds are more frequent--courtesy of web pages that instruct users on how to create viruses and other schemes.
Data Fraud

- Involves:
  - Altering or damaging a company’s data files; or
  - Copying, using, or searching the data files without authorization.

- In many cases, disgruntled employees have scrambled, altered, or destroyed data files.

- Theft of data often occurs so that perpetrators can sell the data.
  - Most identity thefts occur when insiders in financial institutions, credit agencies, etc., steal and sell financial information about individuals from their employer’s database.
Output Fraud

– Involves stealing or misusing system output.
– Output is usually displayed on a screen or printed on paper.
– Unless properly safeguarded, screen output can easily be read from a remote location using inexpensive electronic gear.
– This output is also subject to prying eyes and unauthorized copying.
– Fraud perpetrators can use computers and peripheral devices to create counterfeit outputs, such as checks.
Computer Fraud And Abuse Techniques

- Perpetrators have devised many methods to commit computer fraud and abuse. These include:
  - *Data diddling*

  - Changing data before, during, or after it is entered into the system.
  - Can involve adding, deleting, or altering key system data.
Computer Fraud And Abuse Techniques

- **Data leakage**

  - Unauthorized copying of company data.

- **Denial of service attacks**

  - An attacker overloads and shuts down an Internet Service Provider’s email system by sending email bombs at a rate of thousands per second—often from randomly generated email addresses.
  - May also involve shutting down a web server by sending a load of requests for the web pages. Experts estimate there as many as 5,000 denial-of-service attacks weekly in the U.S.
Computer Fraud And Abuse Techniques

• **Eavesdropping**
  - Perpetrators surreptitiously observe private communications or transmission of data.
  - Equipment to commit these “electronic wiretaps” is readily available at electronics stores.

• **Email threats**
  - A threatening message is sent to a victim to induce the victim to do something that would make it possible to be defrauded.
  - Several banks in the Midwest were contacted by an overseas perpetrator who indicated that:
    - He had broken into their computer system and obtained personal and banking information about all of the bank’s customers.
    - He would notify the bank’s customers of this breach if he was not paid a specified sum of money.
Computer Fraud And Abuse Techniques

• **Hacking**

- Unauthorized access to and use of computer systems—usually by means of a personal computer and a telecommunications network.
- Most hackers break into systems using known flaws in operating systems, applications programs, or access controls.
- Some are not very malevolent and mainly motivated by curiosity and a desire to overcome a challenge.
- Others have malicious intent and can do significant damage.
Computer Fraud And Abuse Techniques

• **Phreakers**
  - Hacking that attacks phone systems and uses phone lines to transmit viruses and to access, steal, and destroy data.
  - They also steal telephone services and may break into voice mail systems.
  - Some hackers gain access to systems through dial-up modem lines.

• **Hijacking**
  - Involves gaining control of someone else’s computer to carry out illicit activities without the user’s knowledge.
  - The illicit activity is often the perpetuation of spam emails.
Computer Fraud And Abuse Techniques

• **Identity theft**

  • Assuming someone’s identity, typically for economic gain, by illegally obtaining and using confidential information such as the person’s social security number, bank account number, or credit card number.

  • Identity thieves benefit financially by:
    – Taking funds out of the victim’s bank account.
    – Taking out mortgages or other loans under the victim’s identity.
    – Taking out credit cards and running up large balances.

  • If the thief is careful and ensures that bills and notices are sent to an address he controls, the scheme may be prolonged until such time as the victim attempts to buy a home or car and finds out that his credit is destroyed.

  • Identity thieves can steal corporate or individual identities by:
    - Watching people enter telephone calling card numbers or credit card numbers or listening to communications as they provide this information to sales clerks or others. May also look for personal information such as checks, credit card statements, bank statements, tax returns, discarded applications for pre-approved credit cards, or other records that contain social security numbers, names, addresses, phone numbers, and other data that allow them to assume an identity.
Computer Fraud And Abuse Techniques

- **Internet misinformation**
  - Using the Internet to spread false or misleading information about people or companies.
  - May involve:
    - Planting inflammatory messages in online chat rooms.
    - Websites with misinformation.

- **Internet terrorism**
  - Hackers use the Internet to disrupt electronic commerce and destroy company and individual communications.
  - Viruses and worms are two main forms of Internet terrorism.
Computer Fraud And Abuse Techniques

- 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**
  - Damage may take many forms:
    - Send email with the victim’s name as the alleged source.
    - Destroy or alter data or programs.
    - Take control of the computer.
    - Destroy or alter file allocation tables.
    - Delete or rename files or directories.
    - Reformat the hard drive.
    - Change file content.
    - Prevent users from booting.
    - Intercept and change transmissions.
    - Print disruptive images or messages on the screen.
    - Change screen appearance.
  - As viruses spread, they take up much space, clog communications, and hinder system performance.
Virus

- **Virus symptoms:**
  - Computer will not start or execute
  - Performs unexpected read or write operations
  - Unable to save files
  - Long time to load programs
  - Abnormally large file sizes
  - Slow systems operation
  - Unusual screen activity
  - Error messages
- They are usually spread by:
  - Opening an infected email attachment or file (most common); or
  - Running an infected program.
Virus

- Virus protections include:
  - Install reliable virus software that scans for, identifies, and destroys viruses.
  - Keep the antivirus program up to date.
  - Scan incoming email at the server level.
  - Deal with trusted software retailers.
  - Have two backups of all files.
  - Do not put diskettes or CDs in strange machines, or let others put unscanned disks in your machine.
  - **Worm**: It is a type of virus that spreads itself over a computer network.
Preventing and Detecting Computer Fraud

• Organizations must take every precaution to protect their information systems.
• Certain measures can significantly decrease the potential for fraud and any resulting losses.
• These measures include:
  – Make fraud less likely to occur
  – Increase the difficulty of committing fraud
  – Improve detection methods
  – Reduce fraud losses