## Basic Terms

### UNIT-I

### Introduction to Cyber Security

Cyber Security Introduction -.Cyber Security Basics:

Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT.or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

What is cyber security?

"Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

OR

Cyber security is the body of technologies,.processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

- The term cyber security refers to techniques and practices designed to protect digital data.
- The data that is stored, transmitted or used on an information system.

OR

Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks.

It is made up of two words one is cyber and other is security.

- Cyber is related to the technology which contains systems, network and programs or data.
- Whereas security related to the protection which includes systems security, network security and application and information security.

## ESSENTIAL TERMINOLOGY

**Vulnerability –**

- Vulnerability - weakness in a system. Weakness that can allow harm to occur.
- Jargon: "Attack surface" – the full set of a system's vulnerabilities

**Common vulnerabilities**

- Untrained users
- Employee sabotage
- Poor authentication implementation
- Poor configuration
- Lack of physical security
- Failure to adequately isolate network traffic
- ... etc

**Threat** – circumstance with potential to cause harm. Threats are possibility of something negative to happen

There are many ways to classify threats

- Nonhuman threats: natural disasters, hardware failures, etc.
- Human threats: spilling a soft drink, entering the wrong data by mistake, intentionally hacking a system
- Malicious vs. non-malicious
- Random vs. directed

**Attack** – exploit of a vulnerability

**Risk**

- Potential of harm (loss) .... From failure/attack of an information system. Risks are the possible outcomes of these exploits
- Likely threats - Fire? Earthquake? Theft? Social engineering? Malware?

**Countermeasure or control** – action or device that removes or reduces a vulnerability

- Defn: "Means to counter a threat"
- Detective – identify when a threat is/has acting(ed) on the vulnerability
  - System monitoring
  - Security alarm system
- Preventive – keep the threat away from acting on the vulnerability

- Actual prevention – physical, environmental, firewall, encryption
- Deterrence – Policies/procedures, training, anti-malware

- Corrective – lessen the impact of the threat
  - Backup/recovery
  - Disaster recovery systems

**Prevent**

- Remove the vulnerability from the system

- **Deter**
  - Make the attack harder to execute
- **Deflect**
  - Make another target more attractive (perhaps a decoy)
- **Detect**
  - Discover that the attack happened, immediately or later
- **Recover**
  - Recover from the effects of the attack

# Essential Terminology

CEH

**Hack Value**

It is the notion among hackers that something is worth doing or is interesting

**Zero-Day Attack**

An attack that exploits computer application vulnerabilities before the software developer releases a patch for the vulnerability

**Vulnerability**

Existence of a weakness, design, or implementation error that can lead to an unexpected event compromising the security of the system

**Daisy Chaining**

It involves gaining access to one network and/or computer and then using the same information to gain access to multiple networks and computers that contain desirable information

**Exploit**

A breach of IT system security through vulnerabilities

**Doxing**

Publishing personally identifiable information about an individual collected from publicly available databases and social media

**Payload**

Payload is the part of an exploit code that performs the intended malicious action, such as destroying, creating backdoors, and hijacking computer

**Bot**

A "bot" is a software application that can be controlled remotely to execute or automate predefined tasks

# Cybersecurity

Cybersecurity Concepts

CSUSM Cybersecurity Education Hub

# Cybersecurity Fundamentals

- What is cybersecurity?
- What are we trying to protect?
- Risk – threats, vulnerabilities, likelihood
- Confidentiality, integrity, and availability (C-I-A) concepts
- What kinds of harm are we trying to avoid?
- How can we avoid that harm?

# What Is ~~Computer~~ Cyber Security?

- The protection of the assets of a ~~computer~~ system
  - Hardware
  - Software
  - Data

# Assets Are…

Hardware
- Computers but also:
  - Medical devices
  - Automobiles
  - Industrial controllers
  - Security systems
  - Household appliances
  - Scientific equipment
  - Tracking/location devices
  - …and more

Software/Network
- Operating systems, applications but also
  - Access control mechanisms
  - Physical Access
  - Location services
  - Network traffic
  - Actions
  - Device identity
  - …and more

Data
- Files, photos, music, databases but also:
  - Location
  - Actions
  - Network identity
  - Access list
  - Payment info
  - Response/Status
  - Monitored activity
  - …and more

# Basic Terms

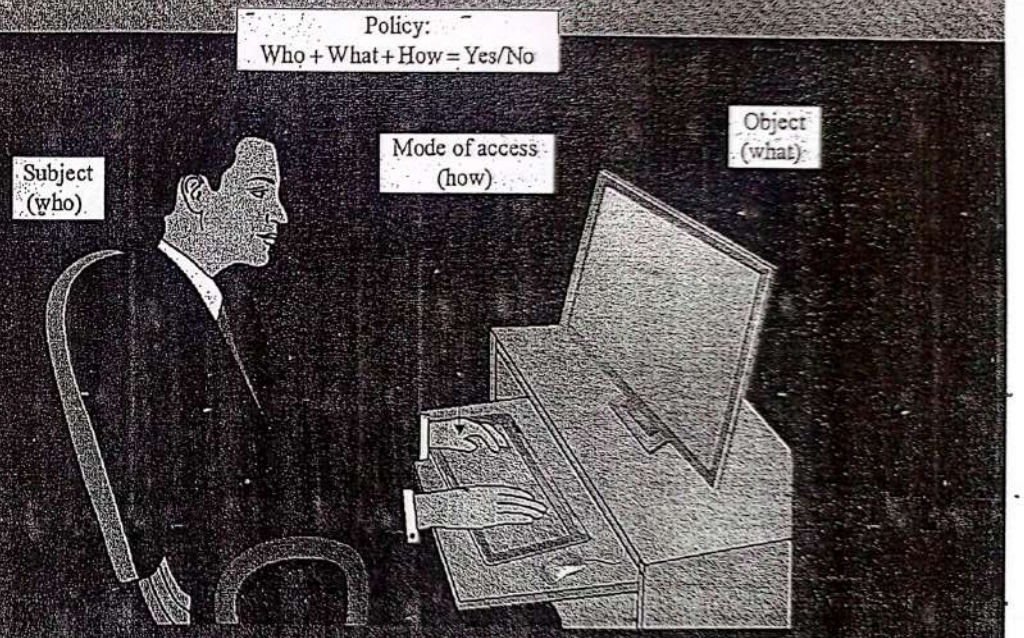
- Vulnerability – weakness in a system
- Threat – circumstance with potential to cause harm
- Attack – exploit of a vulnerability
- Countermeasure or control – action or device that removes or reduces a vulnerability

# C-I-A Triad

- Confidentiality - *Only persons authorized to access information or systems should get access to the information or system.*
- Integrity - *Only those persons or applications authorized to alter the system or information may do so, and alterations are made under controlled circumstances.*
- Availability - *The information or system, along with the applications, and other hosts used to access, store and manipulate it, is available when needed.*
- Sometimes two other desirable characteristics:
  - Authentication – *Confirm identity of a sender/signer.*
  - Nonrepudiation – *Confirm that asserted action can't be denied.*

# Confidentiality

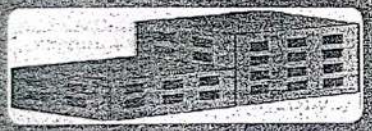
- Both actual data and information about data
- Access to all of it or part of it?
- Unauthorized – both persons and processes or systems
- Generally means viewing/obtaining but not modifying



# Confidentiality

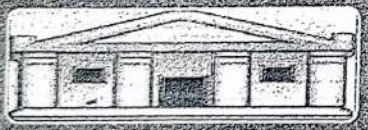
## Personal Data and Information

- Credit card account numbers and bank account numbers
- Social security numbers and address information



## Intellectual Property

- Copyrights, patents, and secret formulas
- Source code, customer databases, and technical specifications



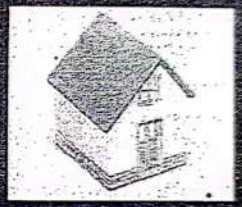
## National Security

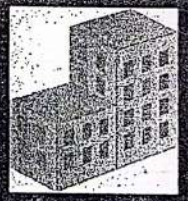
- Military intelligence
- Homeland security and government-related information

# Integrity

- Maintain valid, precise uncorrupted, and accurate information.
  - Word "not" macro
  - Pentium math error
  - Errors
- Purposeful changes to values (accounting, salary)
- Alterations are authorized and intentional

- User names and passwords





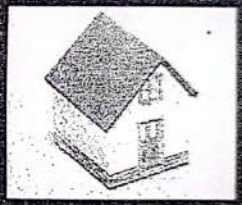
- Patents and copyrights
- Source code

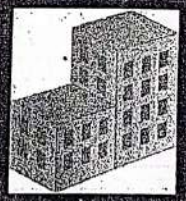
- Diplomatic information
- Financial data

# Integrity

- Maintain valid, precise uncorrupted, and accurate information.
  - Word "not" macro
  - Pentium math error
  - Errors
- Purposeful changes to values (accounting, salary)
- Alterations are authorized and intentional

- User names and passwords





- Patents and copyrights
- Source code

- Diplomatic information
- Financial data

# Availability

- Complex series of topics
- Moves far into operations
  - Backups and recovery?
  - Disk availability – raid, mirroring, cloud services?
  - Personnel and training?
  - Business Continuity/Disaster Recovery?
  - Uptime and "normal" failures?

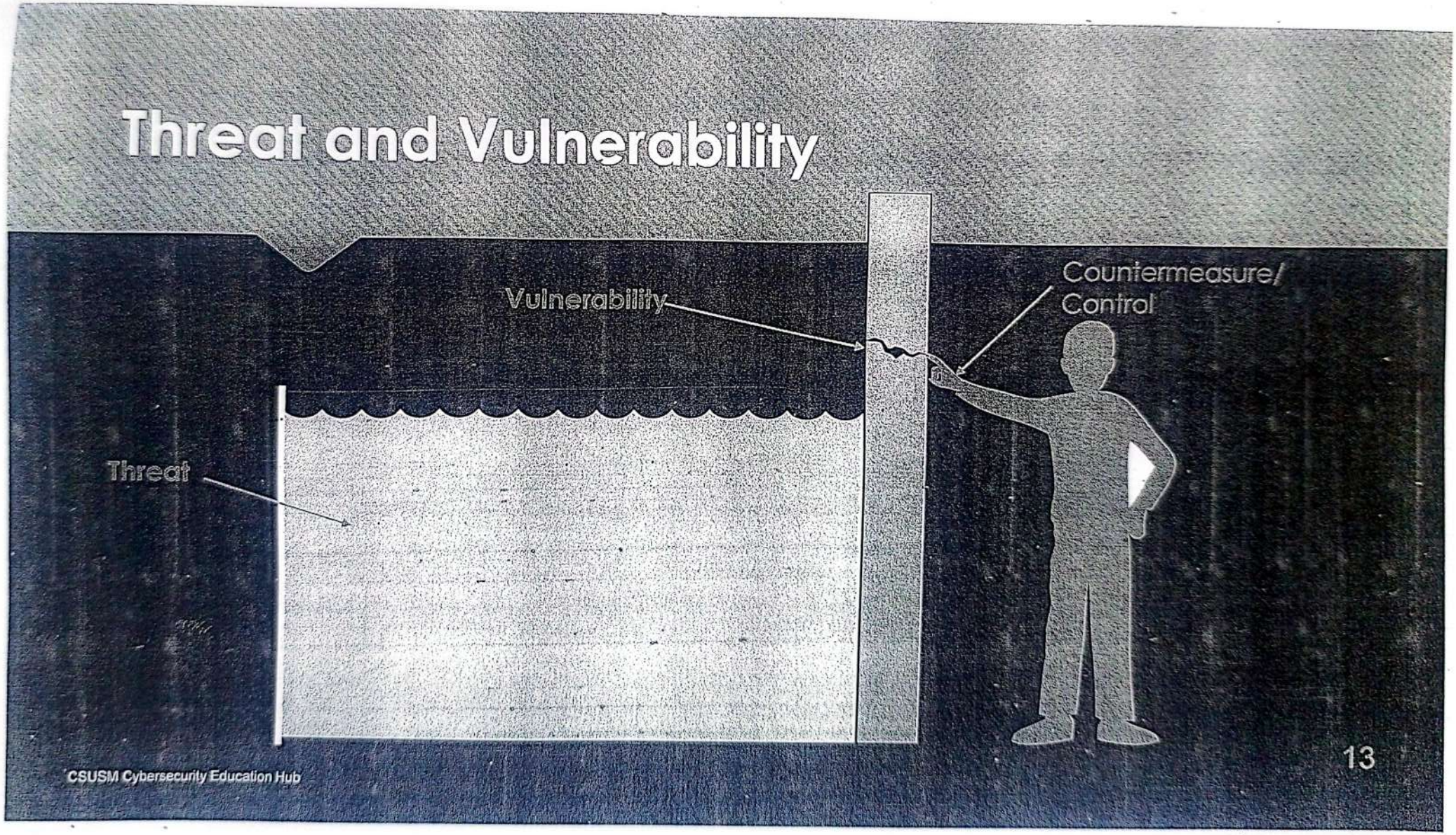
# Harm

- Negative consequence of the attack
- Dependency on value of asset
  - Theft (identity/financial/intellectual property)
  - Loss of privacy
  - Loss (destruction) of asset
  - Organizational operations impact
  - Reputational harm

# Risk

- Potential of harm (loss) …. From failure/attack of an information system
- Likely threats - Fire? Earthquake? Theft? Social engineering? Malware?
- Countermeasures
- Risk transfer
- Value of asset, amount of harm, cost of countermeasure(s)
- Problem:
  - Difficult to assess value
  - Difficult to assess impact (amount of harm)
  - Difficult to identify threats
  - Difficult to assess "likelihood" of threat

# Threat and Vulnerability



# Vulnerability

- Vulnerability - Weakness that can allow harm to occur
- Jargon: "Attack surface" – the full set of a system's vulnerabilities
- Common vulnerabilities
  - Untrained users
  - Employee sabotage
  - Poor authentication implementation
  - Poor configuration
  - Lack of physical security
  - Failure to adequately isolate network traffic
  - ... etc

# Threats

- There are many ways to classify threats
  - Nonhuman threats: natural disasters, hardware failures, etc.
  - Human threats: spilling a soft drink, entering the wrong data by mistake, intentionally hacking a system
  - Malicious vs. non-malicious
  - Random vs. directed

# Harm From Human Threats

- Interception – Someone accessed something to which they had not been granted access
- Interruption - Something became unavailable or unusable
- Modification - Someone changed something they weren't supposed to
- Fabrication - Someone created fake data or records

# Risk and Likelihood

- What's the chance of being invaded by hostile aliens?
- Really, really small?
- **Likelihood** is the chance that a threat will happen
- Effect of being invaded by hostile aliens?
  - Death, destruction...
- Impact is the damage that could occur
- Humans overestimate the likelihood of rare and high-impact events, perhaps underestimate the likelihood of more common, potentially less impactful events. Ex: air travel vs auto travel

# Affecting Likelihood: Method, Opportunity, Motive

- As with traditional crime, a computer attacker must have three things:

| | |
|---|---|
| Method | • Skills and tools to perform the attack |
| Opportunity | • Time and access to accomplish the attack |
| Motive | • A reason to perform the attack |

# Controls/Countermeasures

- Defn: "Means to counter a threat"
- Detective – identify when a threat is/has acting(ed) on the vulnerability
  - System monitoring
  - Security alarm system
- Preventive – keep the threat away from acting on the vulnerability
  - Actual prevention – physical, environmental, firewall, encryption
  - Deterrence – Policies/procedures, training, anti-malware
- Corrective – lessen the impact of the threat
  - Backup/recovery
  - Disaster recovery systems

# Controls

- **Prevent**
  - Remove the vulnerability from the system
- **Deter**
  - Make the attack harder to execute
- **Deflect**
  - Make another target more attractive (perhaps a decoy)
- **Detect**
  - Discover that the attack happened, immediately or later
- **Recover**
  - Recover from the effects of the attack

# Physical Controls

- Locks on doors
- Security guards
- Backup copies of data
- Planning for natural disasters and fires
- Simple controls are often the best
  - Attackers will always look for a weak point in your defenses

# Technical Controls

- Software controls:
  - Passwords
- OS and application controls
  - Encryption, access control methods
- Independent control programs
  - Application programs that protect against specific vulnerabilities
- Development controls
  - Quality control for creating software so that vulnerabilities are not introduced
- Hardware controls
  - Smart cards on satellite or cable television set-top boxes
  - Fingerprint or other biometric readers
- Network
  - Firewalls,

# Procedural Controls

- Humans…
  - Policies, procedures, standards
  - Most important: training and awareness
  - Policy examples:
    - Password composition
    - Prohibitions on sharing
    - Confidentiality agreements
  - Legal protections
    - State/Fed laws
    - Common law