Legal Issues in Information Security

Lesson 1
Information Security Overview

Learning Objective

Recognize fundamental concepts of information systems security (ISS).

- Begin to think about the legal implications of ISS concept and issues
- Definitions and general terms
- Concepts
- Classifications or types of information security
- Different levels of protection for various types of information

What is Information Security?

- Practice of protecting information

What is the primary goal of Information Security?

- To protect 3 aspects of information
  - Confidentiality
  - Integrity
  - Availability

What is a Triad?

- Grouping of three things we generally think about together as a unit

Key Concepts

- Confidentiality, integrity, and availability (C-I-A triad)
- Basic information system security concepts
- Risk analysis and mitigation
- Mechanisms for organizational information security
- Data classifications requiring specialized legal consideration

WHAT IS CONFIDENTIALITY?

- Preventing people who should not have access to data from obtaining it.
- Important at all phases
  - Creation of data
  - Manipulation, summarization, use
  - Analysis
  - Transmission
  - Destroy
- Breaches
  - Intentional
  - Accidential

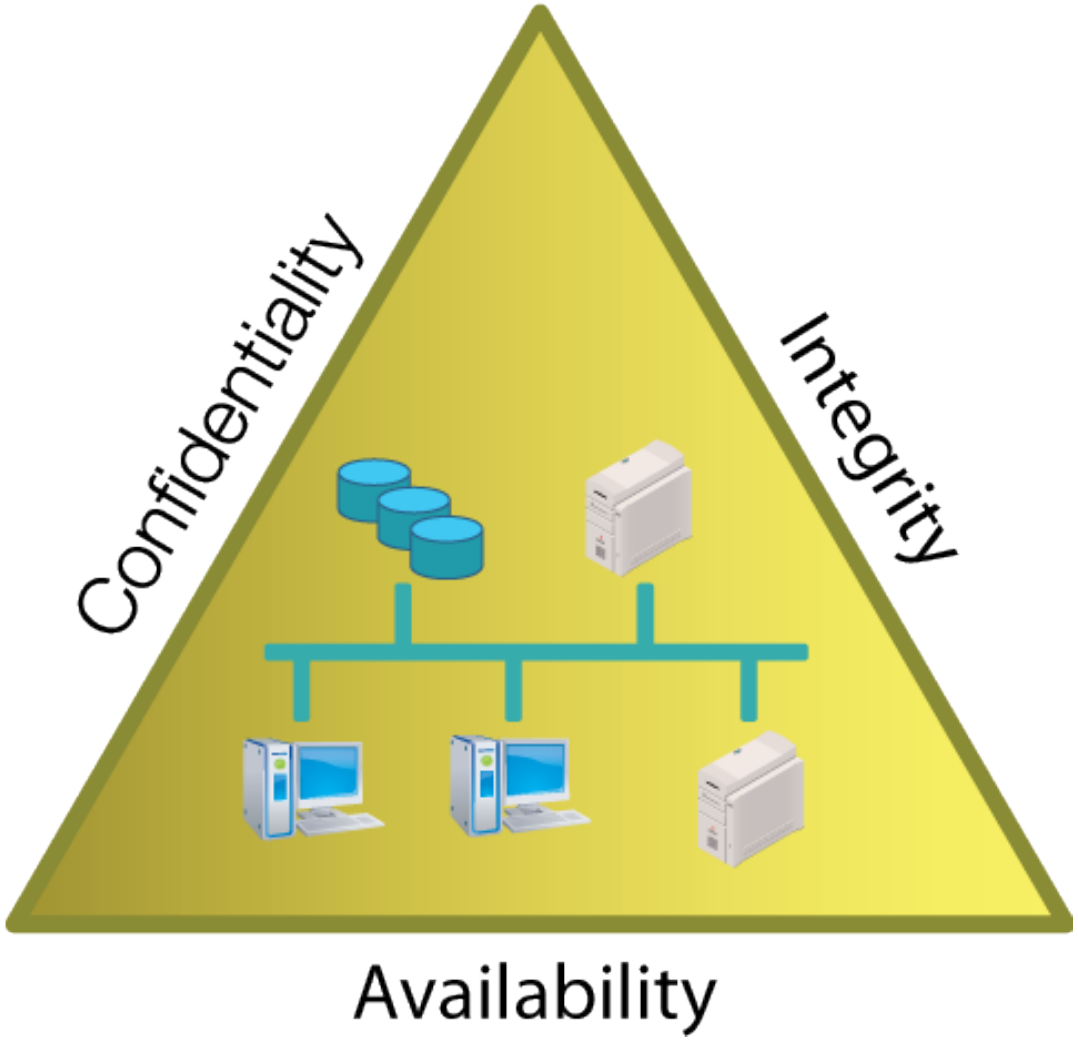
WHAT IS INTEGRITY?

- Means systems and their data are accurate.

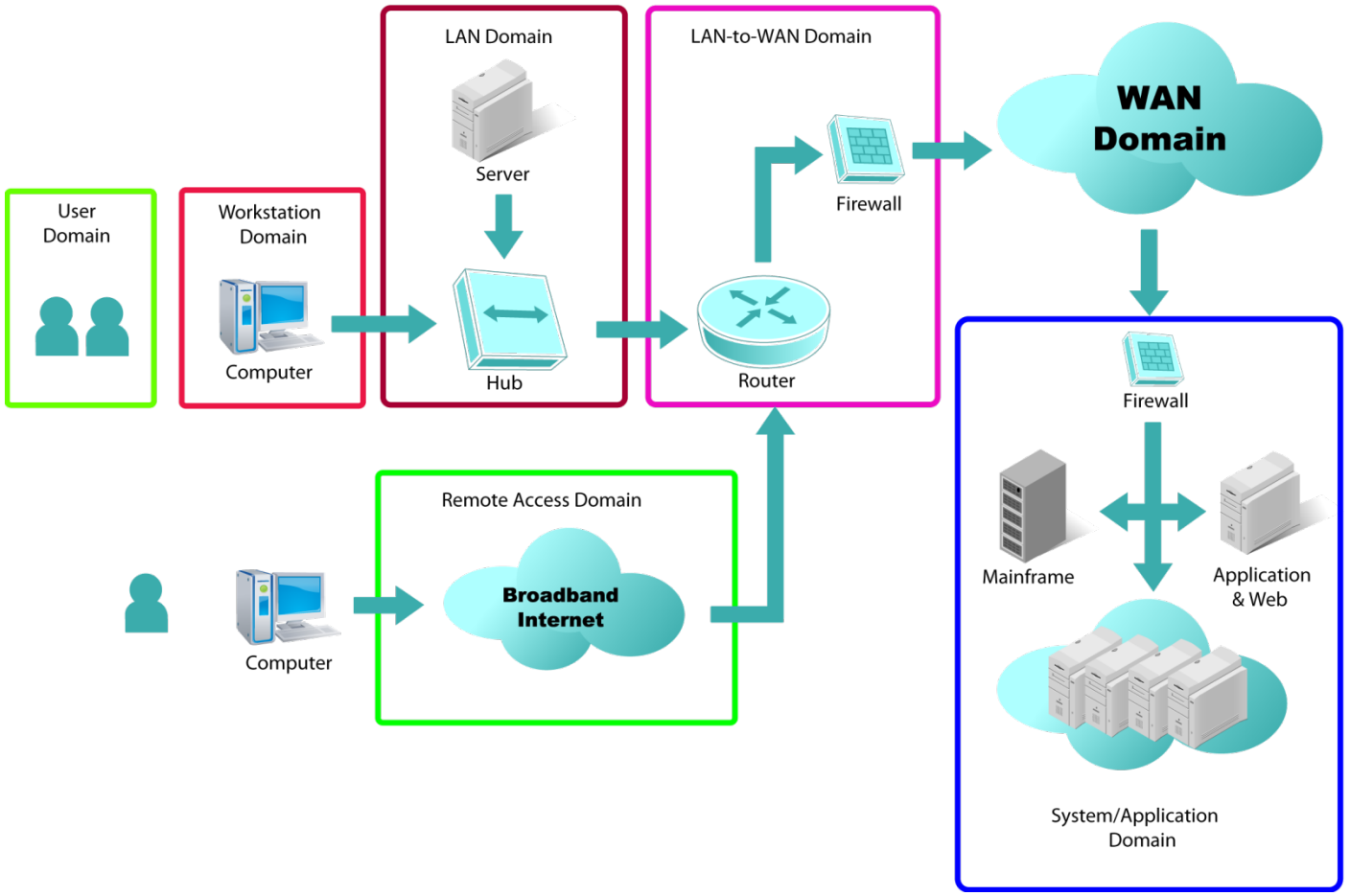
WHAT IS AVAILABILITY?

- Making sure the systems operate reliably and that data is accessible by people with permission when they need it.
- Insures no bottlenecks or slowdowns and that data is available at peak times.
  - Single point failure –Single piece of hardware or software critical to the entire system.

C-I-A Triad



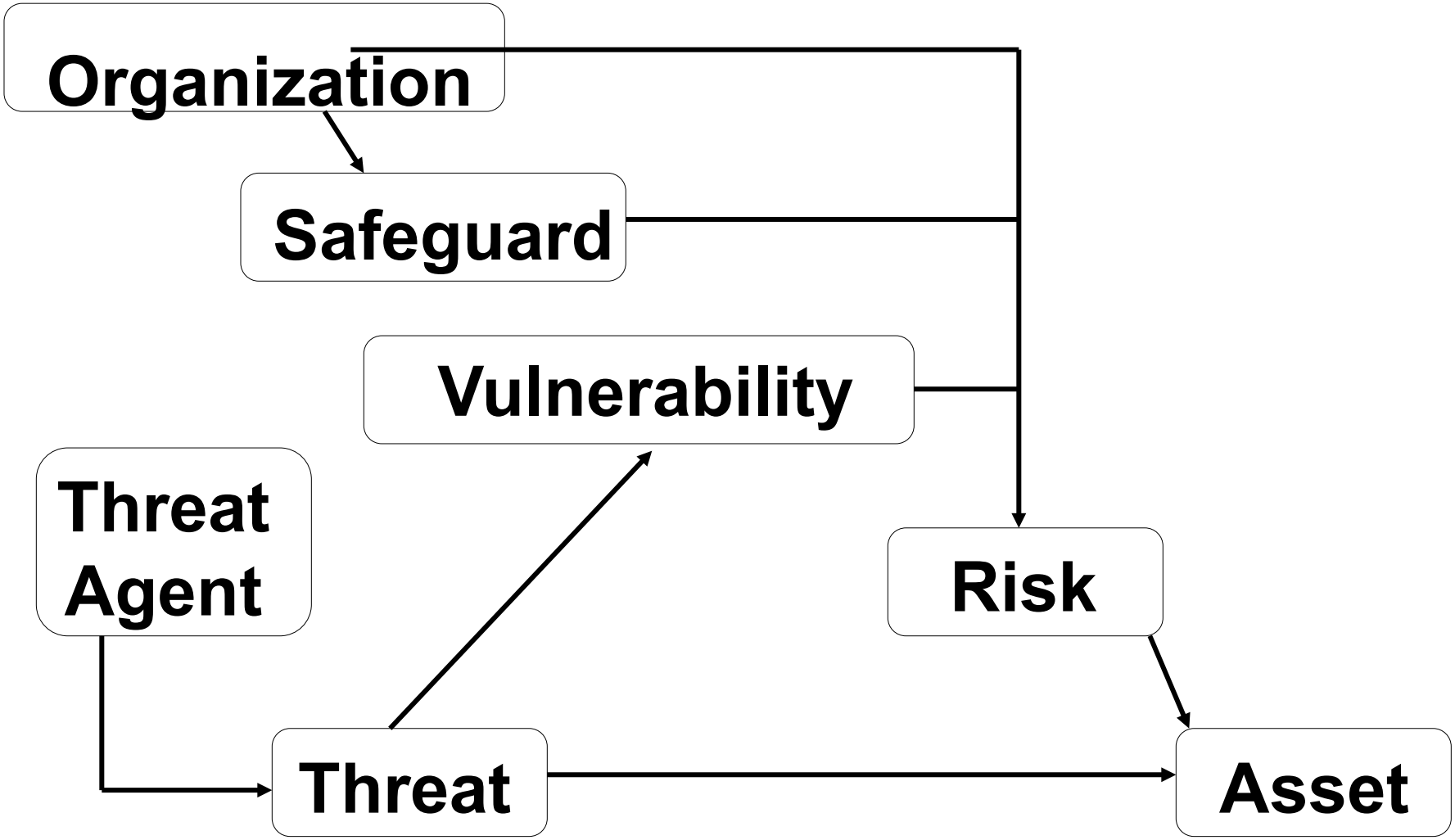
Seven Domains of a Typical IT Infrastructure



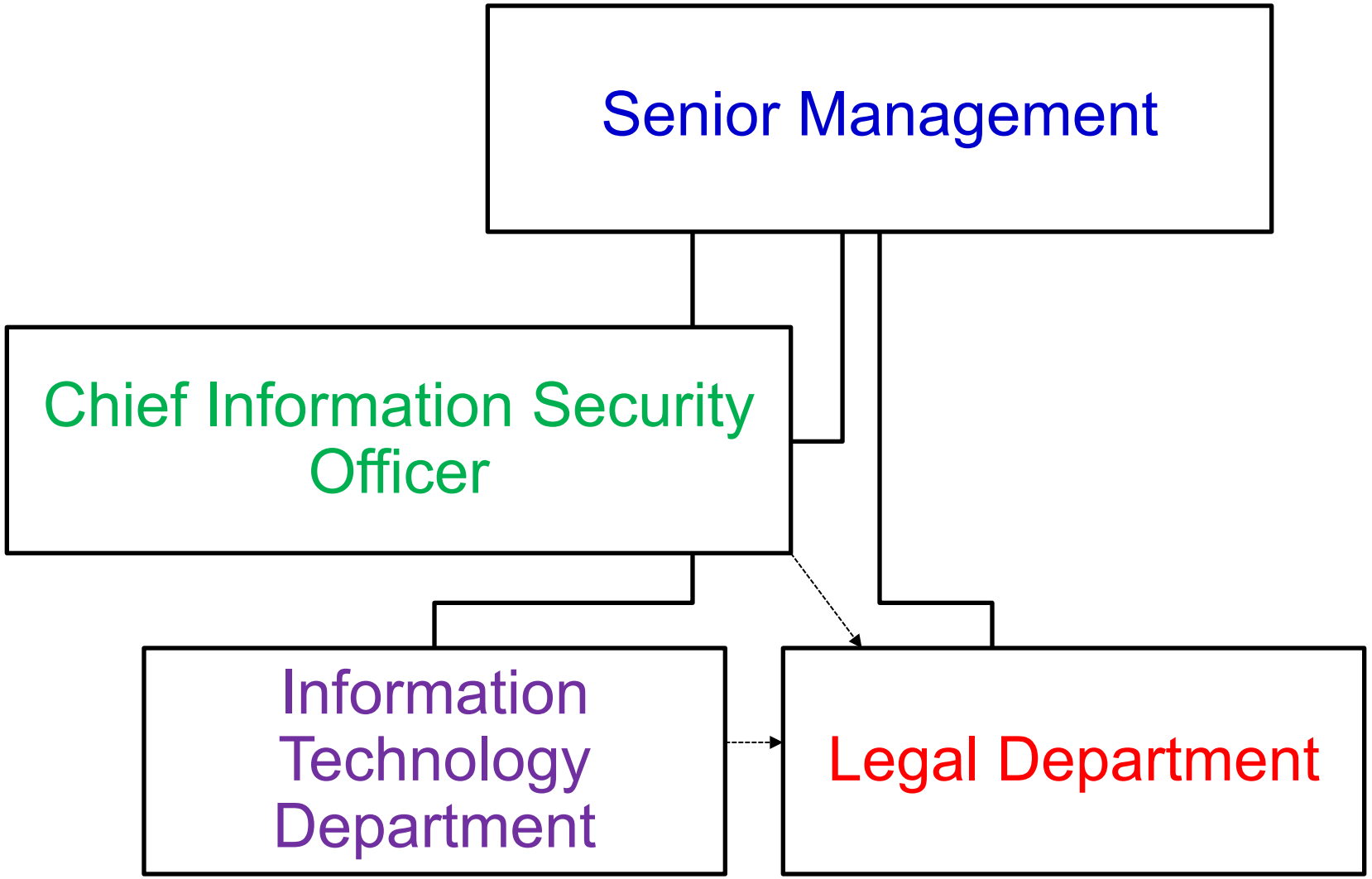
Basic Risk Management Concepts

- Vulnerability ~ asset weaknesses
- Threats – Anything that has the potential to harm the system
  - Threat Agents – Hackers and Malware
- Exploitation – Threats that are carried out
- Mitigation ~ safeguard assets
- Risks ~ The likelihood that a threat will be exploited. Some can be minimized by asset owner
- Safeguards ~ Implemented by an organization as controls used to reduce harm caused by vulnerability and threats.
  - Referred to as “risk mitigation”

Risk Management Process



Roles in Risk Management



Information Security Common Concerns

- Shoulder Surfing
- Social Engineering
- Phishing and Targeted Phishing Scams
- Malware
- Spyware and Keystroke Loggers
- Logic Bombs
- Back Doors
- Denial of Service Attacks

Information Security in Different Contexts

Private-Harmful to organization if disclosed	• High interest in confidentiality
Public-No harm to organization through disclosure	• High interest in availability

Data Classification

Governmental Classification	General Corporate Classification
Top Secret	Corporate Confidential
Secret	Client Confidential
Confidential	Proprietary
Restricted	Public
Unclassified	

Mechanisms for Ensuring Information Security

Legal Mechanisms to Ensure Information Security

- Laws
  - Gramm-Leach-Bliley Act, HIPAA, COPP, FERPA and Many others
- Information Regulations
  - Financial, credit card, health, etc.
- Agencies
  - FTC, Banks, DHHS, SEC, DOE, etc.

Thank you!

Please email questions and/or comments to

Dr. Les Stovall

Leslie.Stovall@ucumberlands.edu