The goal of lnfoSec is to protect assets.

ln the end, security is about maintaining reliable systems (ClA triad).

CIA Triad

* Confidentiality: keeping info private and secret; information not disclosed to unauthorized entities or processes
* integrity: ensuring accuracy and completeness of data over its lifecycle; data cannot be modified in an unauthorized or undetected manner
* Availability: information is available when needed

LAN: a collection of computers connected to one another or to a common connection medium

* The physical part of the LAN Domain includes a network interface card (NlC) which is an interface between the computer and the LAN physical media
* With wireless LANs (WLANs), radio transceivers are used to transmit lP packets from a WLAN NIC to a wireless access point (WAP)

LAN-WAN Domain: the lnternet ingress/egress point; entry/exit point for WAN

* Vulnerable given that TCP and UDP packet headers reveal port #s to the lnternet
* Port scanning, probing network, sensitive data exposure

Frame Relay: a packet-based WAN service capable of supporting one-to-many and many-to-many WAN connections

Weakest Link in Security of lT lnfrastructure: The user; human error

* Malicious, untrained, or careless users (a major risk and threat)
* Do: background checks, rotate access to sensitive systems among staff

VolP: Voice over lP

* An application running on the lnternet
* Uses lnternet's packet switching; allows routing of voice info over any lP-based network(LAN/WAN)
* POTS - Old phone system: PSTN (public switched telephone network)

SIP: Session lnitiation Protocol

* Most commonly used VolP protocol
* A signaling protocol used to support real-time & unified communications
* The protocol used by real-time applications such as lM chat, conferencing, and collaboration
* lt is its own protocol; does not run over a porU there's TCP, UDP, ICMP
* Assigned protocol number 1
* One of main protocols in lnternet Protocol Suite
* Used by network devices (like routers) to send error messages ("service unavailable", "could noteach host or router")
* Differs from transport protocols (TCP, UDP) because it's not typically used in data exchange

Socket: pairing of an lP address and a port number

3-way Handshake (TCP Handshake): (sYN-ACK-SYNACK)

* Creates synchronized connection between a local host/client and server
* Requires both client and server to exchange SYN and ACK packets before data exchange
* The target server must have open ports that can accept and initiate new connections

OSI Model: list with 1 device/protocol at each layer

"Please Do Not Throw Sausage Pizza Away"

"Please Do Not Tell Sales People Anything"

"All People Seem To Need Data Processing"

Risk Assessment

* Risk identification: What could go wrong? Develop scenarios for each threat.
* Risk Assessment:
  + 1. Assess various controls to mitigate risks you identify
  + 2. Select a control strategy that is reliable, scalable, economical, safe, usable
  + 3. Justify your choice by comparing cost of controls against worth of asset
* Inventory Assets: assess loss while you assess risk
* Classify Assets: according to value to business
* identify Threats & Vulnerabilities (to each asset), and compare with proposed controls
* Secure (encrypt) sensitive data
* Pen-test for vulnerabilities in infrastructure

Security Controls: 3 Types:

* Detective control: identify a threat on your system (logging, IDS)
* Corrective control: reduce the effects of a threat (anti-virus, forensics, lR)
* Preventative control: stop threats from coming in contact with vulnerability (firewall, lpS)
* Controls can be physical or logical
* Principle of Least Privilege
* Network segmentation, ACLs

Malware:

Exploit (lock picking) & Payload (the instructions)

Common Attacks: client side & server side

Client-side attacks:

* Social Engineering
* Ransomware
* Attachments
* Web Links

Server-side attacks:

* SQLI
* XSS

Password crackers

* Program that performs a brute force attack, or a dictionary attack
* Dictionary Attacks: use shorter and simpler combos, including actual words

Keystroke loggers

* Records every keystroke into a logfile (encrypted)
* Viruses deliver them
* Police have used them
* Can harvest passwords, personal info, bank info

Business Continuity Plan (BCP):

* Plan for how to handle outages to lT systems, applications, and data access in order to maintain business operations

Disaster Recovery Plan (DRP):

* Written plan for how to handle major disasters or outages, and recover mission-critical systems,applications, and data

Authentication : proving identity

* The act of identifying or verifying eligibility to access specific types of information
* Protecting against fraudulent transmissions by establishing validity of a transmission, message,or originator

Authorization: The granting of right of access to a user, program, or process

Non-repudiation:

* Prevent a party from denying a previous statement or action
* A security service by which evidence is maintained so that the sender and recipient of data cannot deny having participated in the communication.
* Referred to individually as nonrepudiation of origin and non-repudiation of receipt.
* Using Asymmetric Kev Cryptography, you can prove that a particular party did indeed originate a specific message at a specific time
* Asymmetric crypto uses a key pair to encrypt/decrypt
* The originator is the only one who knows one of the keys: it has an irrefutable timestamp
* One party cannot deny having received a transaction
* Other party cannot deny having sent a transaction

Policies, Procedures, Standards, Guidelines (difference between?)

Configuration management

* Process of managing all changes to computer and device configurations
* Unmanaged changes introduce risk (might affect security operations and controls)
* Configuration changes should happen in a controlled process; otherwise this may create new conflicts and security vulnerabilities.
* For security, the goal is to ensure that any configuration changes will NOT cause unintended consequences on security (C.l.A. affected by change?).
* Vulnerability Assessment
* Design Controls/Processes
* Review of Standard Operating Procedures and Policies
* Review of Backup Disaster Recovery/Disaster Recovery Plan
  + This includes a Risk Assessment and BIA
* Configure Management
* Compliance Audit
  + HIPPA
  + 201CMR 17
  + PCI DSS

**Encryption - Asymmetric vs. Symmetric**

Asymmetric Encryption: (2 keys - pub/private; different keys used to encrypt & decrypt)

* Different keys used for encipher and decipher

Symmetric Encryption: (1 secret key; same key used to encrypt & decrypt)

* Same key is used for both encipher and decipher

Hybrid of asymmetric & symmetric (?) (\*Explain in words on exam)

* Encrypt key, then send; get his public key, encrypt AES private key with his public key; send encrypted key to him; decrypt with his private key

Digital signature: ensures non-repudiation

* Use the MD5 or SHA-1 hash to generate a digest from a message
* The output from the hash function (the digest) provides input for an asymmetric key algorithm that also uses a private key as input
* The result of this encryption is a value uniquely associated with the file.
* lt is computationally infeasible to forge and provably related to the identity of the entity that signed the file.
* SIGNATURE GENERATION: Message ) SHA-1 ) Digest ) Asymmetric key algorithm + privatekey + Digest ) Unique Signature
* SIGNATURE VERIFICATION: Message ) SHA-1 ) Digest ) Asymmetric key algorithm + public key + Digest ) Signature (if this signature == the original signature, then it is verified)

The main purpose of the digital certificate is to ensure that the public key contained in the certificate belongs to the entity to which the certificate was issued. Encryption techniques using public and private keys require a public-key infrastructure (PKl) to support the distribution and identification of public keys.  Digital certificates package public keys, information about the algorithms used, owner or subject data, the digital signature of a Certificate Authority that has verified the subject data, and a date range during which the certificate can be considered valid. Without certificates, it would be possible to create a new key pair and distribute the public key, claiming that it is the public key for almost anyone. You could send data encrypted with the private key and the public key would be used to decrypt the data, but there would be no assurance that the data was originated by anyone in particular. All the receiver would know is that a valid key pair was used.

ASA:

* Cisco Adaptive Security Appliance (e.g., Cisco ASA 5500-X Series): most deployed in industry
* A Stateful Firewall

Domain Controller:

* A server that responds to security authentication requests (logging in, checking permissions, ...)
* Domain: concept where user granted access to several resources with single username/passwd

Authentication Server:

* Provides a network service that applications use to authenticate the credentials, usually account names and passwords, of their users.
* When a client submits a valid set of credentials, it receives a cryptographic ticket that it can subsequently use to access various services.

Log Management:

* Gives you analysis data (e.g., diagnostics for car repair)
* "lf it wasn't logged, it didn't happen"
* Log Management Tools: Graylog, Splunk
* Port 514: Svslog: system message logging stream

"lD - 10 - T" == idiot

"PEBKAC" -= problem exists between keyboard and chair

Data Classification Standard:to provide a consistent definition for how an organization should handle and secure different types of data

Denial of Service (DOS): to an attack that uses ping or ICMP echo-request, echo-reply messages to bring down the availability of a server or system

Disaster recovery plan (DRP): defines how a business gets back on its feet after a major disaster like a fire or hurricane

Business impact analysis (BlA): assess assets, then impact

* Prioritizes mission-critical systems, applications, data & the impact of an outage or downtime
* Prerequisite for Business Continuity Plan

Recovery time objective (RTO): is the amount of time it takes to recover and make a system,application, and data available for use after an outage

Demilitarized Zone (DMZ): an exterior network that acts as a buffer zone between the public internet and an organization's lT infrastructure (i.e., LAN-Io-WAN Domain)

* Programmed to distinguish legit packets for various connections
* Only packets matching a known active connection will be permitted through
* Example: Cisco ASA (adaptive security appliance)

VPN: Virtual Private Network

* Extends a private network across a public one (e.g., lnternet)
* Enables users to send/receive data on public networks as if they were on private network
* Users benefit from functionality, security, and management policies of private network
* Allows employees to securely access corporate intranet while out of office