CISSP aide-mémoire

By Éric Allaire, B.Sc., CISSP, P+CP
eallaire@EricAllaire.com

August 9, 2009

Table of contents

References used:

Susan Hansche/John Berti/Chris Hare, *Official (isc2) guide to the CISSP Exam*; 2004
Shon Harris, *all-in-one CISSP certification guide*, 2002;
Shon Harris, Mikes Meyer certification to CISSP, 2002;
Peter H. Gregory; *CISSP for Dummies* , 2003;
Ellen Dutton, *LAN security handbook*, 1994;
Peter H. Gregory, *Solaris security*, 2000;
Ed Tittel/Mike Chapple/James Michael Stewart, *CISSP study guide*, 2003;
www.Infosecuritymag.com
www.cccure.net
www.cccure.org
www.isc2.org

Table of figures:

Special notes

This is not a supplement to your readings, web site browsing, and other studying formulas but intends to be an aide-mémoire prior to your exam. Many hours are required to study the various CKB subjects using web sites, books on-line questionnaires, and forums. The CISSP exam can be very time consuming study, but worth it!

*This document is not a supplement or a substitution to your local/area building codes or local laws.

Distribution agreement:

CISSP aide-mémoire

Domain 1 – Access Controls

The purpose of access control is to protect information and resources from unauthorized logical access to the information.

Definitions:
Subject: is an active entity requesting access to an object or data.
Object: is a passive entity that contains info or data.
Access: ability of a subject to do something such as: read, write, create, execute.
*Access control***:** a security feature that controls how subjects and objects interact with each other.
Granularity: the fine divisions of a component so that it can be fine-tuned which access controls can be regulated.
*Identification***:** the association of some unique or at least useful label to a subject. Ascertains the identity of a subject.
*Authentication***:** proving that the subject is who he claims to be. Something he knows, password; something he has, smart card; something he is, fingerprint.
Authorization: granting access to resources based on criteria list.
Strong authentication (two factor): is the requirement of having two of the three factors of authentication.
Excessive privilege: user or administrator has more privileges then he/she needs for the security of the system.

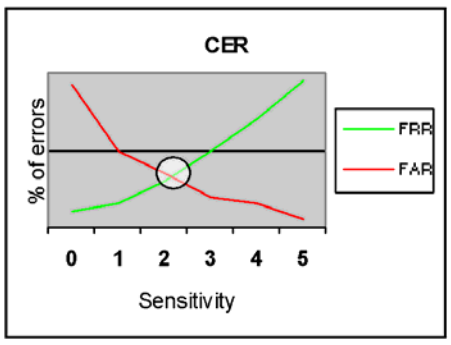
Basic authentication principles
Identification > authentication > authorization =>> resources
The authentication process is done through the combination of those three: something you know (password), something you are (biometrics), something you physically have (cards).
A strong authentication is when least two of the three are used.

Authentication mechanism
*Crypto keys***:** private key or digital signature to prove one's identity. A private key is a secret value in possession by one person. Digital signature is encrypting a hash value with the private key. More secure than static passwords.
Passphrases: a sequence of characters is typed; software transforms them into a virtual password. More secure than a password because it is longer and easier to remember
Memory cards: it holds the authentication information. Just like an ATM. Added cost of reader, card creation and maintenance.

Types of password:
Cognitive passwords is when fact based information is used to verify identity. A question is asked to the subject and he answers. Mother's name, pet name, favorite idol. It is easy to remember.
One-time password: it is good only for one authentication, uses a token.
Synchronous one-time password generator: synchronized with the authentication service by using time or an event to authenticate. Time /event driven. Encrypted using time value.
Asynchronous one-time password generator: same thing but uses a challenge response.
Passwords characteristics: cheapest, least secure (easy to shared, written down), most widely used authentication technology.

Biometrics
Biometrics is physical attributes for authentication through unique physical personal attributes, most accurate, sophisticated, and very expensive. It is not very accepted by society. Biometrics stores information in a database or on a smart card. It can be a 1-to-1 matching process, where 1 feature is compared/contain to 1 specific file (retina match to a smart card). Or, it can be a 1-to-many matching process, where 1 feature is compared to a large database with many items.

Error types:
Type I: false rejection (False Reject Rate or false negative) is when a good subject is not authenticated
Type II: false acceptance (False Accept Rate or false positive) is when an impostor is authenticated.



Crossover Error rate (CER):

Crossover Error rate (CER):
The CER is the point where rejection and acceptance intersects. If system A has 3 persons out of 100 rejected then type I errors = 3%. The lower Crossover Error Rate (CER) is, the more accurate the biometry is.
Example: System A has 1 out of 100 type I errors = 1%
System A has 1 out of 100 type II errors = 1%
CER = 1

Types of biometrics (respond time/CER): fingerprints (5/5), finger scan (selective finger print), palm scan, hand geometry(4/2), iris scan (2/0.5), hand signature dynamics (7/?), keyboard dynamics, voice print (12/10), facial scan, hand topology.

Access control models:
Discretionary Access Control
DAC: discretionary access control solely granted based on the authorization granted by the owner. Uses ACL.
Mandatory Access Control
MAC: Mandatory Access Control is based on the security clearance of subject and classification of object, in other words based on labels. The OS determine access.
Role-Based Access Control (RBAC)
It's also called a non-discretionary access control. It allows access to objects based on the role the user holds within the company. Administrator assigns to a role certain rights and each user is placed in a role. Oracle works that way.
Lattice-based Access Control:
Every pair of elements is compared to roles, their permission and clearance levels with the sensitivity level of the object to determine access level.
Ruled based
Security policy based on global rules imposed for all subjects. MAC is an example. Rule-based access techniques are based on specific rules that indicate what can and cannot happen to an object.
Restricted interfaces
Menus: the administrator specifies the menu available to the user.
Shells: the administrator specifies the menu available to the user through OS command.
Database view: limited by table view.
Physically constrained:
limiting keypad or touch buttons like an ATM.
Control matrix
Table of subjects and object specifies their access relationship.
Capability table
Capability table specifies the access rights a certain subject has to an object.
ACL
ACL are used to authorize a subject to access an object and they are bounded to the object.
Content-dependent access control
Access to objects can be determined by the sensitivity of the content within the objects. As an example a user may have access to a payroll DB but another user cannot.

Access controls attributes: Groups, physical location, logical location, time of day, transaction type.

Access control administration
Access control administration – centralized
One entity, senior management make access rights policies admin enforce it, RADIUS, TACAS+, DIAMETER

RADIUS: Remote Authentication Dial-in Service is an authentication protocol that authenticates and authorizes. It provides a handshakes protocol. User dials-in to communicate. RADIUS server holds a database of users and credentials. Communication between client and server is protected. Steps: 1) user dials-in (PPP) 2) RADIUS prompt for credential. 3) User supplies credential. 4) RADIUS client sends credential to RADIUS server. 5) RADIUS server accepts, reject or challenge. 6) If authenticated, RADIUS client access to network.

DIAMETER: is a protocol designed better then RADIUS. It provides users authentication with more than just SLIP and PPP, it provide protocols for PDAs, laptops or cell phones. It includes a better message transport, proxying, session control and higher security transactions.

TACACS+: Terminal Access Controller Access Control System is an authentication protocol to authenticate remote users. It splits authentication, authorization and auditing features. It is a Cisco protocol.

Access control administration – Decentralized
Control is given to people closer to the resource. Access control is processed by several entities.

Single Sign-on technology: is a technology where the user presents their credential once, the user can then access all resources across accredited network. It is less administration, user is centralized, user only needs to remember one set of credentials. SSO uses scripts or a directory services (LDAP). The various protocols are: Kerberos, Sesame, Thin clients.

Kerberos: 1)user authenticates to the Authentication Server (AS), 2) AS sends initial ticket, 3) user requests to access an object, 4) each time user requests to access an object the Ticket Granting Serv (TGS) creates new ticket with session key from the Kerberos Distribution Center(KDC), 5) user accesses the object. Downfalls are single point of failure, secret key stored with users, dictionary attacks, KDC must be available, by default not encrypted.

Sesame: Secure European Applications Multi-vendor Environment. 1) user sends credentials to AS, 2) AS sends token back to user, 3) user with token requests to the Privilege Access Server (PAS) a Privilege Access Certificate (PAC), user accesses the object server.

Thin-client: a dumb terminals network where each terminal requests tickets from the mainframe.

Steps of controlling access:
1) Decide on the model, 2) decide on the technology/techniques, 3) how is access be managed (centralized, decentralized, hybrid)

Access control administration – Hybrid
Combines centralized and decentralized admin methods. One entity controls what users accesses and individual users are allowed to decide who can access their own resources.

Access control categories:
Technical Access Controls:
System access: computer control access
Network architecture: network constructed to provide and enforced trough logical controls.
Network access: Network devices are used to control what entities enter and leave a network.
Auditing: controls through tracking activities of users and systems.

Physical Controls:
Network segregation separates the network from others.
Perimeter security of the network's surroundings.
Computer Controls provides a physical control to protect. Like removable HD.

Administrative controls:
Are those that use policies standards as a way to enforce controls.

Access control characteristics are preventive detective, corrective, deterrent, recovery, and compensation. Often these controls can be combined.

Intrusion detection
There are two types of IDS, networked based and the host-based. The networks based listen to a segment of the network and the host-base listen to a host only.

IDS can be *ruled-based* where a sequence of user activities or triggered by activities that compromise the system states.

Statistical/anomaly-based function by comparing a known historical pattern of intrusion to a behavior within the system.

Signature-based is compared with a signature database.

Attacks to access
See attacks on telecommunication services

Attacks on passwords
Dictionary attacks is a program with a list of possible passwords
Brute force: is a program that tries different characters, not words.

Domain 2 - Telecom and net security

The purpose of this domain is to segregate non-trusted networks using devices, architectures, and protocols to protect the trusted network.

Definitions:
LAN: is a network that allows sharing resource in a small area.
MAN: backbone that connect business to WAN.
WAN: bounded by geographical region.
Intranet: network within the organization's walls.
Extranet: network outside of the organization's wall connected to business partner.
Downstream liability: responsibility to partner to not introduce a vulnerability on the extranet.
EDI: Electronic Data Interchange, exchange data between partners in a standard format.
Broadband: more than one channel.
Base band: one channel.
Asynchronous: A type of transmission in which each character is transmitted independently without reference to a standard clock; uses stop and start bits.
Unicast transmission: one-to one relationship.
Multicast: one to many relationships.
Broadcast: one to all relationship.
MAU Multistation Access Unit: is a central hub to which all the computers are connected (ring formation).
Beaconing: detection of a problem then sending a beacon frame.
Tunneling: refers to encapsulation of protocol A within protocol B, such that A treats B as though it were a data link layer. Tunneling is used to get data between administrative domains, which use a protocol that is not supported by the Internet connecting those domains. PPTP and L2TP are tunneling protocols

CISSP aide-mémoire

War dialer: program that dials numbers until a modem is found.
Phreaker: Phone hacker that specializes in telephone frauds.

TCP/IP
Transmission control protocol/internet protocol is a suite of protocols that rule the way data travels from one device to another. It is divided in two TCP and IP. The TCP is a reliable and connection oriented protocol. The IP is a connectionless protocol that routes data. IP works at the network layer providing routing services. IP does not provide a reliability that each packet has arrived. TCP ensures that each packet reaches their destination using handshakes. Ver6 is 128bit address ver4 is 32. TCP and UDP have over 65,000 ports, 0-1023 well-known ports.

User Datagram Protocol
UDP is a connection-less protocol which does not handshake, doesn't sequence its packets, doesn't communicate back to the source, but is faster than TCP and good to provide video streaming.

Cabling and data transmission types
Cables:
Coaxial cable is a surrounded copper wire, more resistant to interference than CAT, more expensive. Broadband or base band Twisted-pair made of copper wires shield (STP) or unshielded (UTP). Each pair are twisted to a different spin per inch to prevent interference, it is inexpensive. It has a high resistance to flow of signals, radiates energy and easy to tap. CAT 1 to 7. 1 = voice, 2 = data 4MPS, 3 = 10MPS token, 4 = 16MPStoken, 5 = 100mps, 6 = 155 MPS, 7 = 1GPS.

Electro Cable issues white noise, attenuation, and cross talk.

Fiber optic uses light. It is high speed, hard to tap, very secure, not subject to interference.

Fire issues: it is important to use the right fire rated cable. Plenum space cable meet specific fire code and it is made of fluoropolymers. The non-plenum cables are made of PVC.

LAN technology
Network topology
Network topology is the physical arrangement of systems and devices usually forming a star, ring, tree, mesh (partial, full), or bus (linear, tree) pattern.

Media access technology
Media access technology is how systems communicate over the media and access method is how the computer gains access to a shared network object. Here are some technologies:

Ethernet is a LAN sharing technology that uses broadcast and collision domains, uses CSMA/CD, full duplex, used on STP, coax;

Token ring technology developed in 70's, all nodes are connected to a central device (MAU), the rings extend out the station and back to MAU one token on network at one time;

Token passing is a media-access-control strategy in which a sequence of 24-bit known as a "token" is passed from node to node. The node that currently holds the token has control of the communication channel.

Polling is a communications access method used by some computer/terminal systems whereby a "master" station asks many devices attached to a common transmission medium, in turn, whether they have information to send.

Protocols stack:
A set of rules enabling computers or devices to exchange data with one another with as little error as possible. The rules govern issues, such as error checking and data compression methods.

Address Resolution Protocol (ARP). A TCP/IP protocol used for resolving local network addresses by mapping an IP address (i.e. a MAC address) to a physical address. It is not use for routing. ARP poisoning is the unauthorized alteration of ARP table.

Reverse Address Resolution Protocol (RARP). The Internet protocol that diskless host uses to find its Internet address at start-up. RARP maps a physical (hardware) address to an Internet address.

Internet Control Message Protocol (ICMP). The protocol used to handle errors and control messages at the IP layer. ICMP is actually part of the IP protocol. ICMP report routing failures, test node reachability, increase routing efficiency.

Simple Network Management Protocol (SNMP), an Internet standard that defines methods for remotely managing active network components such as hubs, routers, and bridges.

Simple Mail Transfer Protocol (SMTP), the standard by which electronic mail messages are communicated over the Internet.

Other protocols: LDP, NFS, TFTP, FTP, Telnet, BootP.

Network devices and services

Devices	OSI layer	Function in order of security controls
Repeater	Physical	Device used to amplify and/or regenerate attenuated signals.
Bridge	Data link	Connects two or more networks and forwards packets between them. Bridges read and filter packets and frames. Bridges do not require IP addresses and will pass broadcast traffic.
Router	Network	Device that determines the next network point to which a data packet should be forwarded towards its destination. The router is connected to at least two networks and determines which way to send each data packet based on its current understanding of the state of the networks it is connected to. Routers create or maintain a table of the available routes and use this information to determine the best route for a given data packet.
Brouter	Data, network	Device which bridges some packets (i.e., forwards based on data link layer information) and routes other packets (i.e., forwards based on network layer information). The bridge/route decision is based on configuration information.
Switch	Data	Similar to a hub, in that it provides a central connection between two or more computers on a network, but with some intelligence. (A switch operates on Layer 2 (or above) of the OSI 7 layer model and a hub operates at Layer 1.) Whereas for a hub any message received at the hub is broadcast to all the attached computers, with a switch it is sent only to the destination computer and is not visible to other attached devices. This does not prevent "broadcast" messages from being sent to all attached devices.
Gateway	Applicati on	A computer system for exchanging information across incompatible networks by translating between two dissimilar protocols.
Virtual LAN	Top physical	A logical, not physical, group of devices, defined by software. VLANs allow network administrators to re-segment their networks without physically rearranging the devices or network connections.
Firewalls	Apps, sessions, network	A computer device and/or software that separates a Local Area Network from a Wide Area Network and prevents unauthorized access to the Local Area Network through the use of electronic security mechanisms such as IP filtering, address re-mapping, etc . More on firewalls.
IDS	Session	Intrusion detection system which is either host-based or network-based or application IDS. An IDS monitors all of the network traffic from a central point (network-based), generally inside the firewall, and reports on traffics that seem containing malicious traffic. Needs updates, just like a virus scanner. IDSs comes in various detection types: Knowledge/signature-based, Behavior/rule-based (state and model based) or statistical.
IPS	Session	Intrusion Protection Systems works very similar to IDS, except that IPS will usually take certain course of action to prevent or stop the malicious activities. IPS systems are able to detect malicious activities using the characteristics of the behavior and not just an attack signature. This line of defense can help prevent forecast attacks.
Data Diode	Physical	

What is a difference between firewall and IDS? The firewall is an intrusion blocking system that opens certain ports and blocks all the others. The IDS is an intrusion detection system that detects all packets on the network in real-time and blocks illegal sessions. The firewall inevitably deteriorates system performance because it filters all network traffic, whereas the IDS does not affect network traffic at all and that it accepts the input only without an output.

Firewalls:
A method of guarding a private network by analyzing the data leaving and entering. Firewalls can also provide network address translation, so the IP addresses of computers inside the firewall stay hidden from view. *Packet-filtering firewalls* (layer 3) use rules based on a packet's source, destination, port or other basic information to determine whether or not to allow it into the network. More advanced, *stateful packet filtering firewalls* (layer 7) have access to more information such as; conversation, look at state table and context of packets; from which to make their decisions. *Application Proxy firewalls(layer 5)*, which look at content and can involve authentication and encryption, can be more flexible and secure but also tend to be far slower. *Circuits-level* proxy looks at header of packet only, protects wide range of protocols and services than app-level proxy, but as detailed a level of control. Basically once the circuit is allowed all info is tunneled between the parties. Although firewalls are difficult to configure correctly, they are a critical component of network security.

Demilitarized zone (DMZ) is an area of a network, typically between the internal corporate network and either the external Internet or a partner, vendor, or client, usually between firewalls, providing some service or services.

Bastion:
An exposed gateway, host or set of machines that provide non-secure services between the protected, local network and the Internet, and resides on the public segment.

Architecture type	characteristics
Dual-homed Untrusted net > firewall > trusted net > host (Single tier)	Single computer with 2 NICs, one to the trusted network and the other to external untrusted network
Screened host Untrusted net > router > firewall > host (Two tier)	Router filters traffic before it is passed to the firewall then the firewall passes it to the host directly.
Screened subnet Untrusted net > router > semi trusted net > firewall > trusted net > host (Three tier)	External router filters traffic before it enters the DMZ. Traffic heads towards the internal network then goes through a firewall and another router.

Firewall placements:
Firewall can be placed to create a DMZ allowing a buffer zone between two networks. The bastion is the entry point & exit point out of the system. It is a system tightly locked with no necessary services running such as user accounts or user files.

Firewall principles:
When using firewalls, security is focused at one point. Having a distributed approached will increased security. Firewalls present a potential blockage to flow of traffic taking away quick access to services to lawful users. Most firewalls don't protect against most viruses passing trough e-mail, the virus scanner does. Firewalls don't protect again inside attackers, IDS does. Remote access using modem is not protected using firewalls. Those were some of the downside of firewalls. Having two firewall administrators available to ensure one is always available. Remote access for administrators should use strong authentication over an un-trusted. The only account on the firewalls should be those administrators with privilege set to make changes only. The firewall configurations should get backed up periodically with read only media. A second firewall should be ready to go on-line quickly. Any irregularity should be recorded and reported. Configured so the "no reply" on port scans or pings. If a firewall ever goes down the new one should be re-set and re-implement necessary controls, re-run integrity controls after reconfiguration. Most vulnerability is caused from missed configuration (default settings). Ensure to have a security policy dictating regulations away from the firewall default. The firewall should be set to fail-safe not fail-open. A full backup before being put into production (day zero backup).

Data diode:
A physical layer hardware device called a **Data Diode** is used to create an air gap between the secure network and the general-purpose network. The Data Diode then permits data to flow in only one direction - from the general-purpose network to the secure network. (I am writing a paper on the data diode)

Connectivity protocols:
Connectivity protocols
Several protocols assume access from outside the LAN, this connectivity uses modem and dial-up devices.
SLIP: Serial Line Internet Protocol, replaced by PPP, it is asynchronous serial connections. Unlike PPP it doesn't have header and data compression, error correction, support different authentication methods, encapsulate other protocol other than IP, and support other types of connections other than asynchronous.
PPP: it encapsulates over a serial line for dial-up connectivity. Authenticated using PAP, CHAP, EAP.

Authentication protocol:
PAP: Password Authentication Protocol used by remote users, authenticates after PPP is established, credentials are sent in clear text, vulnerable to sniffing, man-in-the-middle and attacks.
CHAP: authentication protocol that sends a challenge response, credential have encrypted values, periodically sends a challenge to protect man-in-the-middle attacks, password is not sent over the wire.
EAP: Extensive Authentication Protocols: enables more possibilities to get different types of identifications and authorization information from users.

Tunneling protocols
VPN: provide remote access to an organization's network via the Internet. VPNs sends data over the Internet through secure (encrypted) "tunnels." It is encrypted using PPTP, IPsec and L2TP. Each frames is wrapped and encapsulated within a second frame. L2TP: (layer 2) Layer Two Tunneling Protocol - A secure protocol used for connecting Virtual Private Networks over public lines (Internet).
PPTP: (layer 2) point-to-point tunneling protocol.
IPsec: (layer 3) Internet Protocol Security. IPSec uses encryption technology to provide data confidentiality, integrity, and

authenticity between participating peers in a private network. IPSec provides two choices of security services: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data.
S/WAN: Secure Wide Area Network, a project involving RSA Data Security and a number of other companies. The goal is to ensure interoperability between all their IPSEC implementations to let all the customers communicate with each other securely. Firewall to firewall.

Remote access methods and technology
Remote access covers several technologies to give access to a LAN. Most of the time an ISP is the gateway to the network. Remote access in many organizations offers work home opportunities. Remote access is usually done trough a Network Access Server (NAS/client side). The NAS (authenticate and authorize) will then use PPTP or L2TP to establish the link.

Remote network access
The RAS (Remote Access Server/server side) can be configured to call back or accept call from ID-caller number. Here is intricacy to configure a RAS: modem/server installed in a central point protected by firewall separating to internal network; revised access right and users yearly; remote access policy enforced; use VPN (it's encrypted) avoid war-dialer using over three or four rings before answering phone.

Wireless technology:
Many networks use wireless devices to provide communication. Spread technology places different types of data to the signals at a specific allotted data frequency spectrum. Two types of spectrum exist Direct Sequence Spread Spectrum (DSSS) and Frequency Hoping Spread Spectrum (FHSS). The 802.11 use 2.4 GHz along with other devices like microwave it creates a dirty range.

Wireless Application Protocols
WAP is a set of protocols to standardize the wireless technology. Similar to TCP/IP, web-based technology. Like WML Wireless Mark-up Language, WAP uses WTLS Wireless Transport Layer Security which is the session and transaction protocols and with transport layer together. WTLS provides 3 classes of security Class 1, anonymous authentication; 2, server authentication; 3, two-way client/server authentication.

SSID: Service Set ID is required when wireless devices need to authenticate to AP. The SSID provides authentication but can be shifted.

OSA Open System Authentication and SKA Shared Key Authentication: there are two wireless methods of authentication OSA is not encrypted and data transmission is in clear. On the other hand SKA encrypts only the payload not the headers/trailer using Wired Equivalent Privacy (WEP), which use symmetric algorithm RC4 40bit or 104bits. The payload is encrypted.

Network services
DNS: Domain Name System (or Service), an Internet service that translates domain names to or from IP addresses, which is the basis of Internet addressing.
NAT: Network Address Translation – circuit level gateway translates multiple IP addresses on a private LAN to one public address used on the Internet.

Telecommunications protocols and devices
FDDI: (Fiber Distributed Data Interface) - A standard for transmitting data on optical fiber cables at a rate of around 100,000,000 bits-per-second (10 times faster Ethernet, about twice as fast as T-3).
SONET: High-speed fiber-optic network constructed in rings so data can be re-routed in the event of a fiber cut.
Dedicated link: permanent point-to-point link.
CSU/DSU: A hardware device that provides a digital interface to high-speed line connections and acts like a digital modem. The CSU connects the network to the transmission line; the DSU converts data for transmission by the CSU and controls data flow
ISDN: Integrated Services Digital Network and is a system of digital phone connections which allows voice and data to be transmitted simultaneously across the world using end-to-end digital connectivity. There are two basic types of ISDN service: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). BRI is a basic service is intended to meet the needs of most individual users. PRI is for users with greater capacity requirements.
DSL: Digital Subscriber Line. This technology uses ordinary copper telephone lines to provide Internet speeds ranging from 1.5 to 9 Mbps - speeds that are 30 to 50 times faster than a regular 56-kbps dial-up modem. DSL also allows users to receive voice and data simultaneously, since the signal is carried on a higher frequency than normal telephone communications. The user must be no more than 2.5 miles from the telephone central.
Cable modems: provides up-to 50mbps using local cable.
Frame relay: uses packet-switching technology to allow multiple company and networks to share the same media.
X.25: This standard defines the interconnection of packet-switching networks and their associated computers or terminals. These types of networks make efficient use of the telecommunications networks by taking the data generated by a computer or a remote terminal and chopping it up into small identified packets and then looking for the most efficient way of sending this information to its destination.
ATM: Asynchronous Transfer Mode. International standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells.
SMDS: Switched Multi-megabit Data Service is a high speed, packet switching technology used to enable clients to extend their LAN: Connectionless, bandwidth on demand has caught the IT community.
SDLC Synchronous Data Link Control: used dedicated permanent physical links, used by IBM main frames as bit synchronous protocol evolved as the HDLC.
HDLC High Level Data Link Control: derived from SDLC bit oriented synchronous with full-duplex P-to-P and multipoint connections.
Multi-service Access Technology: is fast, flexible, cost efficient technology to data, voice, video, which allows various types of protocols to access it like VoIP, VoATM, VoFR.
X400: standards of message handling.
X.509: encryption of public key.

Attacks related to telecomms
Impersonation: A technique by which one process can take on the security attributes of another process, as when a server process impersonates a client process to complete a task involving objects to which the server does not normally have access.
Packet modification: the alteration of packet during transmission. Hashes, digital signatures, are countermeasures
Flooding: sending more data than the system can handle; ping of death, mail bombs. Countermeasures is packet filtering and patch
TCP sequence number: Attackers predict TCP sequence numbers to gain access to a system. Encryption and look for ACK storms to prevent it.
TCP hijacking: spoofing the TCP address. Challenge responses, encryption and ACK storm to counter this attack.
Web spoofing: using the web pretending to be someone else. Impersonating, masquerading, and mimicking are forms of spoofing.
DNS Poisoning: false resource DNS table. Countermeasure is using DNCSEC.
Login spoofing: fake login table. Countermeasure is trusted secure channel user and system.
SYN attack: taking advantage of a TCP connection request (SYN) a spoofed IP address is sent to the target. The attackers send many SYN to the target to slow it down or give in DoS.
War driving: physically driving around with a listening device to catch wireless packets.
Cell cloning: each cell has an Electronic Serial Number (ESN) to ID the phone and a Mobile Identification Number (MIN), which the phone number assigned to it the ESN. The attackers intercept the numbers and copy it to another phone.
Private Branch Exchange (PBX) threats: PBX located on the organization's property, a phreaker can enter the system to reroute calls, reconfigure the switches, or enable access to free long distance calls.
Replay attacks: An attack in which the attacker records data and later replays it in an attempt to deceive the recipient.
Smurf: A malicious attack where the hacker sends a large number of spoofed ping packets to broadcast addresses, with the intent that these packets will be magnified and sent to the spoofed addresses. This has exponential possibilities, depending on how many hosts respond.
Fraggle: the same as Smurf attack but uses UDP
Teardrop: sending smaller size packet or fragmented packets
DoS: Action(s) that prevent any part of an information system from functioning in accordance with its intended purpose. Usually flooding a system to prevent it from servicing normal and legitimate requests.
DDoS: same as DoS but uses several systems to flood.
Password sniffing: Attack in which someone examines data traffic that includes secret passwords in order to recover the passwords, presumably to use them later in masquerades
IP spoofing: An attack whereby a system attempts to illicitly impersonate another system by using its IP network address. Routers and other firewall implementations can be programmed to identify this discrepancy.
Dumpster diving: going through trash to find information
Wiretapping: attaching a special device to the line so that the person can secretly listen to a conversation.
Scanning attack: hacking technique checking ports to reveal what services are available in order to plan an exploit those services, and to determine the OS of a particular computer.

Domain 3 – Security management

This domain investigates and analyzes the current state of security of information finding loopholes in the systems then applying the proper amount of counter-measures, if needed.

Security definitions:
Vulnerability is the weakness of the mechanisms that protect the information.
Threat agent: is the vector that may carry an attack.
Threat is the thing that causes the damage.
Risk is likelihood that the threat agent will use a vulnerability. Two types: total risk and residual risk after countermeasure.
Exposure is the actual occurrence of an incident by the threat agent.
Countermeasure is what was done to lower the threat to enter.

Example: Once a week a hacker place a virus on a server through a weak port. The virus is the threat, hacker is the threat agent, the vulnerability is the open port, the risk is once a week (very likely), and the exposure is the incident itself. A counter measure is applied against a vulnerability when a virus scanner is updated.
Social engineering is tricking someone into giving up confidential information using social skills. Counter measure: employees training.

Vulnerability x Threat = %Risks

CIA triad is the company gain of security objectives. There are three distinct types of threats.
Threats against **confidentiality**, which is the ability to ensure a necessary level of secrecy, privacy, or sensitivity being enforced through data processing. Threats against the **integrity** is how accurate and reliable information or systems are against possible unauthorized modifications. Threats against the **availability** of information is how the information is accessible to users.

Due care is doing what is right to protect assets and employees through policies before the threat occurs and **due diligence** is the actual research of possible threats or steps that a normal person/employee will take to prevent a threat. Basically the data owner (executive) must be diligent to care about the assets.

Control types:
In general, control types are certain functions to restrict various company assets by the data owner.

Administrative
Administrative controls are the development of policies, standards, procedures, and guidelines. It indicates how servers should be installed, annual security awareness education for employees, implementing a change control program.

Technical
Technical controls consist of logical mechanisms, intrusion detections, encryptions, and firewalls.

Physical
Physical controls involve the restriction towards the facility itself. Removing floppy disk and hard drive, locking computers, using IDS, air environment control.

Security model:
A security model is the framework of all administrative, technical, and physical controls. First the security policy is built, then implementations procedures, standards, and guidelines that support the policy. The goals of the models are: **operational** goal that deals with day-to-day activities. **Tactical** goals, which are mid-term goals. **The strategic** goal is a long-term goal, the final objective that includes operational and tactical goals. Planning the security models using these goals is called the **planning horizon**.

Risk Management
Is the process of identifying, assessing, and reducing the risk to an acceptable level and implementing mechanism to keep the acceptable level in place.

Risk Analysis
It is the method of identifying assets and their value, identifying and associating risk to those assets, the possible damages, and implement the necessary cost-effective countermeasure.

IT security specialist and representative from each department conduct the risk analysis. The team will identify assets and assign value to them. The IT administrator plays a big part of the process but does not compose the whole team. The team is composed of people from various departments, because IT staff do not see the whole picture.

The sign-off letters ensure business managers have responsibility of their decisions.

Assigning value to the assets:
An asset can have a quantitative (# or $) measure and a qualitative (rated 1-10, Delphi method) measure assigned to it. The values are assigned to get a better picture of the cost/benefit analysis, help the selection of safeguards and evaluation for insurance purposes; some insurance companies require this practice to provide coverage. Several factors are considered when estimating the values: The book value which is the complete cost to get the asset including developing it and maintaining it. The market value or price others are willing to pay. The liability is asset if compromised, capital lost from lost of operation and productivity, and cost to replace the asset.

Calculation in steps
Annualized Loss Expectancy
Asset Value x Exposure Factor (EF) = Single Loss Expectancy (SLE)
The asset value is the value assigned during the risk analysis. The Exposure Factor (in%) is percentage of asset loss prediction caused by identified threat(s) a value obtained from a chart on exposure research.
SLE x Annualized Rate of Occurrence (ARO) = Annual Loss Expectancy (ALE). The (ARO) is the frequency of occurrence of a threat. It is calculated between the ranges of 0.0 (never) to 1.0

(always). So if the possibility of a fire to occur is once per every 20 yrs then the (ARO) is 0.05 (1/20yrs).
Example:
Step1: Understanding the goals of the company
Step 2: Asset evaluation needing protection. Building = $430,000; Cust. Info. = $200,000; trade secret = $430,000; data = $12,000.
Step 3: Identifying risk and treat agent to assets. Building = Fire, employee; Cust. Info. = stolen, employee; trade secret = exposed, hacker; data = corrupt, software.
Step 4: Estimate the full potential loss of each risk. It is figured out using the (SLE)
Step 5: Estimate the probability and frequency of risk using the Annualized Loss Expectancy

Asset	Risk	Asset Value	Potential loss (SLE)	Annualized Frequency (ARO)	Annual Loss Expectancy (ALE)
Build	Fire	$430k	$330k	.05	$46k
Cust info	Stolen	$200k	$200	.50	$100k
Trade secret	Viewed	$430k	$400k	.80	$320k
Data	Corrupt	$12k	$12k	.50	$ 6 k

This table gives a good idea of the assets needing protection and the amount of resources to invest.

Step 6: Suggest counter measures and remedial. Cost/benefit comparisons, dealing with risks.
Comparisons of cost to safeguard to cost of potential loss.

Asset	Cost of assets	Cost of safeguard	Residual	Y / N	Deal risk
Building	$430k	$ 5 k	1 %	Y	Transfer
Cust. info	$200k	$12k	25%	must	Reduce
Trade Secret	$430K	$500K	100%	N	Accept
Data	$25k	$25k	100%	N	Reject

Value of counter measures = ALE before counter measures – ALE after – annual cost of countermeasure.

The countermeasures should be upfront apparent but the mechanisms should be hidden. The cost should encompass human intervention costs, cost to support it, hardware cost.

Accepting the risk the company has looked at the possibility to protect but it is ineffective to protect or not profitable. On the other hand *rejecting* the risk the company is not looking into protecting the assets and it is being negligent.

Security Policy
Organizational policy is formed by business needs, laws, regulations, and standard of due care. *Issue specific policies are* issue to control in more details an area of the organization. *System specific policies focus* on the information systems themselves like the servers or back-ups.

Policy background: after understanding the risk management develop security policies with strategic and tactical goals. They point out what role IT sec has. The policy needs to pay attention to user behavior. Define reporting relationship and structure. And, the management needs to give proper support to the policy. If the management knows about a risk and is not doing anything then they accept the risk. If the owner is not looking at the risk then they are rejecting it.

Standards compulsory rules that lay down how the IT systems are employed. *Baseline* is the minimum level of security required. *A guideline* is the framework that staff is supposed to follow if standards aren't applied. *Procedures* are the step-by-step actions to reach the task goals.

Basically the policy, written at a high level, is the "what is" and procedures, standards and baselines are the "how to".

Layers of responsibilities:
Data owner is a member of the management who is responsible for the protection of the info. *Data custodian* (IT staff) is responsible to the maintenance of the info, which does not belong to them. *User* is the individual that uses the info and is responsible for its confidentiality, integrity, and availability.

Data classification
Data classification: the principle behind data classification is to specify the level of confidentiality, integrity, and availability. The value of a data must be identified, organized according to disclosure, loss, or sensitivity, and then each classification should get particular security controls.

Commercial:	Military:
Confidential	top secret
Private	secret
Sensitive	confidential
For intern use	sensitive but unclas
Public	unclassified

Classification criteria:
Usefulness of data, Value of data, Age of data, Damage level if data is disclosed or modified, law and liability of protecting the information, Who should maintain the data, Where data should be kept, Who should be able to reproduce the data, What data should require labels and special labels.

Data classification procedures:
Identify the responsibilities, criteria to classify, data owner classifies the data, identify the level of security and controls, indication of how to transfer information, identify declassification, security awareness program, enforcement.

Employee management:
Appropriate employee management is very important. Hiring procedure (back ground credit check) and termination (user account disable) must be outlined. The employees should get regular security awareness training to maintain their info protection practice.

Attacks against confidentiality it is where unauthorized disclosure of information occurs. Causes: object reuse, deleting pointer, data hiding keystroke monitoring, emanation. To protect against this type of attack is to offer control zones, white noise, tempest equipment.

Domain 4 – Apps & Sys dev

The purpose of this domain is to apply security through the life cycle of software use.

Definitions:
Malware: A generic term (MALicious softWARE) describing any form of malicious software; eg, viruses, Trojan horses, malicious active content, etc.
CASE: computer aided software engineering
JAD: Joint Analysis development. Teamwork
RAD: Rapid Application Development
Prototyping: Builds prototypes and limited production runs to test branded concept prior to final production
Waterfall: a method of software dev that uses discrete phase formal review and documentation before moving to next steps.
Spiral model: just like waterfall but has built in risk analysis
Split knowledge: more than one person knows.
Software escrow: Using two pieces of software to form the whole.
OOP: Object Oriented Programming
Message: A collection of data that is ordered according to the rules of a given protocol suite, such that it is intelligible to the sending and receiving software.
Instance: An object of a particular component class. Each instance has its own private data elements or member variables. Component instance is synonymous with object.
Delegation: The ability of an object to issue a message to another object in response to a message. Delegation can be used as an alternative to inheritance.
Inheritance: An object-oriented programming technique that allows the use of existing classes as bases for creating other classes.
Residual data: data that is left after it's been deleted
Data mining: The process of analyzing data to identify patterns or relationships.
Data warehousing: A data warehouse is a collection of data gathered and organized so that it can easily by analyzed, extracted, synthesized, and otherwise be used for the purposes of further understanding the data.
Cell suppression technique is used against inference attacks in hiding information where a statistical query produces a very small result set.
Perturbation addresses inference attacks and involves making minor modifications to the results to a query.
Partitioning involves splitting a database into two or more physical or logical parts.
Remote access Trojan is a software installed on the target and allowing control of the computer to gain information and control.
Mobile code is script or a program that rides on the network (internet) and runs on the client computer.

Project development security
Software development should be planned and managed during the life cycle of the system. There are several security issues that must be dealt with during the planning phase of the development. Dealing with security issues is very expensive later in the development. There are different models with the fundamentals following components:
Project initiation is the conceptual phase that defines the projects, identify security requirements, risk analysis, set security framework, and the SLA (Service Level Agreement).
Functional design analysis and planning defines security requirements, outlines the security check points, and risk analysis.
System design defines security specification, updates the plan, formal method developed.
Software development is writing programming codes implementing security, unit testing.
Installation / test / implementation component testing, user acceptance testing, data proof, system installation, documentation, certification and accreditation.
Operation and maintenance software maintenance using SLA, re-certification, audit and test security components.
Disposal closes the cycle of software dev moving data to another system.

Administrative controls:
Change control prevents confusion and centralized management of the project. Changes are made at source code net production codes. The steps of change controls are: request of change is formally made, analyze request, develop implementation and costs, review security, record changes, submit change request, develop changes, re-code segments, link code changes to the formal control request, submit testing request, make version changes, report changes to management. Changes should be submitted, approved, tested and recorded.

Administrative duty should be separated such that the programmer should not be the only one performing testing. The operation should not have source code and programmer should not work on production software. Once the software is released it should be released to the library from there to production. The responsibility of proper testing performed is management responsibility. The knowledge and access should be split amongst persons to minimize damage of one person.

Software developing models
Waterfall, spiral JAD, RAD, CASE, prototyping

Object-Oriented programming
Classic programming approach is a method in series where one unit gets computer after the other. OOP is divided in module, called object, where each module can be reuse at any time. The benefits of OOP over classical is it increases speed of software dev, saves money and time, re-usable modular, self-contained, resembles business activities.

OOP structures are made of *Classes* that are the characteristic and attributes of the objects. The *object* encapsulates the characteristics. The objects are re-usable. The commands are performed by the *method*. The object communicates using *messages*. The data are hidden (data hiding) from all other program outside the object.

Polymorphism is when two objects send the same message but have different results. In other words objects respond to the same command in a different way. It is possible because objects belong to different classes.

Abstraction is the ability to view unnecessary details so that important ones are examined and reviewed. It looks at the whole picture instead of concentrating on small details. It allows separation of conceptual aspects of the system.

Polyinstantiation repeatedly produces more detailed objects by populating variables with different values. They develop other versions of the object using different values for the variable. That ensures that lower classified info does not access data at a higher classification.

Application threat
Object re-use all sensitive data to be erased before it is accessed (residual data). *Garbage collection* is a process that should unallocate committed storage when not needed. *Trap door* is way to bypass access controls. *Buffer overflow* is when data flow is wider than allocated memory. *Covert channel* when object uses resources as a communication channel that was not intended.
Data diddling: modification of data before it is entered.
Supper zapper: old IBM utility used to bypass normal system controls such as auditing access controls.
Information warfare: attack on the nation's infrastructure.
Pseudo flaw: a backdoor purposely enter in the OS or program to trap an intruder.

Distributed computing
Meaning that all resources are installed on individual computers. The client/server provides the services.

ORB Object Request Broker manages communication between client/server in the distributed environment. The ORB locates and distributes objects across network.

CORBA allows different applications written in different languages to communicate. Standard set of interfaces and APIs for system to communicate with various ORB.

Other distributed systems are Component Object Model (COM), which allows for simple inter-process communication between objects; and Distributed Component Object Model (DCOM) using Globally Unique Identifier (GUID), allows objects on different systems to communicate.

OLE: Object Linking and Embedding. An object is a block of code that may be embedded in another program. For example: OLE allows an Excel file to be embedded in a Word document.

ActiveX: A set of technologies that enables software components to interact with one another in a networked environment, regardless of the language in which the components were created. ActiveX is built on Microsoft's Component Object Model (COM). Currently, ActiveX is used primarily to develop interactive content for the World Wide Web, although it can be used in desktop applications and other programs. ActiveX controls can be embedded in Web pages to produce animation and other

multimedia effects, interactive objects, and sophisticated applications.

JAVA applets: Small Java programs that are embedded in a Web page and run within a browser, not as a stand-alone application. Applets cannot access some resources on the local computer, such as files and serial devices (modems, printers, etc.), and generally cannot communicate with other computers across a network. Java script is different than JAVA programming which resembles C++.

CGI: Common Gateway Interface, an interface that connects the Web with other software and databases. CGI defines how data is passed from a server to a CGI program and has nothing to do with the programming language itself. Hence CGI programs can be written in a variety of languages (such as C, Pascal, Perl, etc).

Cookies: are small text files that Web sites place in your computer to help your browsers remember specific information. For example, they might store your passwords and user IDs. They are also used to store your preferences for content or personalized pages. Most shopping carts use cookies. These allow to choose items and leave the virtual store, then return later and find that all the items are still in your shopping cart. Cookies are also used to build a profile of which sites you visit and which banner ads you click on. Advertisers use this information to deliver targeted ads directly to your computer. Some sites save your preferences on the cookie itself. Other sites assign users ID numbers or encoded passwords and keep records of your preferences at their end. Some sites use temporary cookies (called session cookies) that are deleted when you exit your browser. Others place persistent cookies, which stay on your hard drive for long periods.

Databases
A database is interrelated data stored in a way to allow users/applications to simultaneously access and modify data. Database management allows the database to enforce control, data integrity and redundancy, and allows different data manipulation.

Database are divided in models; hierarchical data models (data presented in a tree, with highest being "root"), relationship (data presented in columns/rows and tables are linked within the DB), distributed (several database, logically connected, complex back-up), network database network (many-to-many relationship hierarchically across network). Structured Query Language (SQL)

Database Definition:
Relation: logical or natural association of two or more objects.
Attribute: construct whereby objects or individuals can be distinguished
Degree: number of columns in a table.
Cardinality: The number of rows in a table
Tuple: A row in a table.
Element: data in a row
Schema: A collection of logical structures of data, or schema objects. A schema is owned by a database user and has the same name as that user.
View: An alternative way of looking at the data in one or more tables. A view is usually created as a subset of the columns from one or more tables.
Primary key: A column that uniquely identifies a row in a table.
Foreign key: A column in a table that matches the primary key in another table.
Data dictionary: A set of database system tables that contain the data definitions of database objects.
Meta-data: data about data. Data that provides information about, or documentation of, other data managed within an application or environment.
Data warehousing: Process of combining data from various sources.
Data mining: tools to identify trends using info held in data warehousing and creates metadata.

Data communicates using Open Database Connectivity (ODBC). ODBC allows applications to communicate with different types of databases. It is the interface between the apps and database drivers.

Database securities:
A concurrency problem is when two users update data at the same time. Software locks can prevent it.
Trusted front-end is an added security which add layers of protection subjects and objects.
Aggregation is an act of combining info from separate sources for which users might not have all access rights.
Inference is the ability to derive info not explicitly available, in other words gaining info from known data.

Artificial intelligence (AI)
Expert systems: applications of artificial intelligence techniques to perform decision-making tasks based on a programmed set of rules and logic within specific subject areas. Examples include insurance underwriting or investing which frequently employ case-based reasoning or semantic analysis. View records related to this term.

Artificial Neural Network: An artificial neural network uses artificial intelligence to learn by past experience and compute. A computer program consisting of a set of simple parallel units or "neuron" with connections between them. The neurons change state according to some simple function of the inputs received and the associated with their connections. In an ANN, knowledge is embodied in the connection weights. An ANN can be used to compute a function by forcing the input units into a given state and observing the state of the output neurons.

Types of attacks (malware)
Malware: A generic term (MALicious software) increasingly being used to describe any form of malicious software; eg, viruses, Trojan horses, malicious active content, etc. the way to detect those malware is to look for change in file size, unexpected disk access, change in file time stamp, decrease in HD space, change in checksums, sporadic system activities.
Viruses are subdivided in categories:
Macro virus: (from macro software), boot sector virus, compression virus (initialized on file decompression) stealth virus (hides its footprint), polymorphic (makes copy and then changes them), multi-party (infects boot sector and file system), self-garbling virus (garble own code to escape detection).
Worms: A computer program that can make copies of itself. Unlike the virus they do not need others to replicate.
Logic bomb: Unauthorized computer code, sometimes delivered by email, which, when executed, checks for particular conditions or particular states of the system which, when satisfied, triggers the perpetration of an unauthorized, usually destructive, act.
Trojan horse: An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

Domain 5 - Cryptography

The purpose of this domain is to protect CIA using mathematical means such as cryptography, hashing etc.

CIA goals:
Confidentiality is a technique that ensures that the intended party only sees the message.
Authenticity is a technique which verifies who actually sent the message, signed. No confidentiality.
Confidentiality and authentication is achieved secure and signed.

Definitions:
Cryptography: The art/science using mathematics to secure information creating a high degree of trust in the electronic realm.
Cryptology: The branch of mathematics concerned with cryptography and cryptanalysis.
Confidentiality: Assuring information will be kept secret, with access limited to appropriate persons.
Authenticity: The property of genuineness, where an entity is what it claims to be.
Integrity: Assuring information will not be accidentally or maliciously altered or destroyed.
Non-repudiation: Ensures that information cannot be disowned.
Cipher: method that encrypts or disguises text.
Algorithm: A procedure or formula for ciphering.
Cryptanalysis: The art and science of breaking encryption or any form of cryptography.
Key clustering: when two different keys generate the same cipher text, the same plaintext.
Hash: A short value calculated from digital data that serves to distinguish it from other data.
Scytale: tool used to perform a transposition cipher, consisting of a cylinder with a strip of paper wound around it on which is written a message.
Caesar cipher: alphabetical shifting method. 13 substitutions.
Vigenere cipher: A polyalphabetic substitution cipher involves the use of two or more cipher alphabets. There is a one-to-one relationship between each letter and its substitute. There is a one-to-many relationship between each letter and its substitutes.
Vernam cipher: one-time pad.
Key Zeroization: is the complete destruction of any remnants of a key.
Split knowledge: encryption keys separated into two parts, each is not revealed to the other.
End-to-end encryption: message is encrypted from one end to the other during transmission no matter what route the packets takes.
Link encryption: the entire circuit is encrypted with hardware or software, bulk encrypted.

Cipher principles:
Kerckoff's principle: The system must be practically, if not mathematically, indecipherable; 2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience; 3. Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents; 4. It must be applicable to telegraphic correspondence; 5. It must be portable, and its usage and function must not require the concourse of several people; 6. Finally, it is necessary, given commands of its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

Key escrow: data security measure in which a cryptographic key is entrusted to a third party. Under normal circumstances, the key is not released to someone other than the sender or receiver without proper authorization. Key escrow systems can be considered a security risk if the user put access to information into the hands of an imposter holding the cryptographic key; but, key escrow systems are used to ensure that there is a backup of the cryptographic key in case the parties with access to key lose the data through a disaster or malicious intent.

Basic encryption methods
Substitution
Substitution cipher: A *simple* substitution is one in which each letter of the plaintext is always replaced by the same cipher text symbol. In other words, there is a 1-1 relationship between the letters of the plaintext and the cipher text alphabets. Caesar cipher is an example. Bytes levels

Monoalphabetic substitution is a single substitution, and polyalphabetic substitution uses several alphabet substitutions.

Transposition
Transposition cipher: A **transposition cipher** encodes a message by reordering the plaintext according to some well-defined scheme. Mathematically, it can be described as applying some sort of bijective function to the positions of the characters. The receiver decodes the message using the reordering in the opposite way, setting the ordering right again. Mathematically this means using the inverse function of the original encoding function. Bytes and bit level.

Block symmetric
Block cipher: symmetric-key encryption algorithm that transforms a fixed-length block of *plaintext* (unencrypted text) data into a block of *cipher text* (encrypted text) data of the same length. This transformation takes place under the action of a user-provided secret key. Decryption is performed by applying the reverse transformation to the cipher text block using the same secret key. The fixed length is called the block size, and for many block ciphers, the block size is 64 bits. In the coming years the block size will increase to 128 bits as processors become more sophisticated.

Stream
Stream cipher: is a cipher in which the input data is encrypted one bit (sometimes one byte) at a time. Sometimes called *state ciphers* since the encryption of a bit is dependent on the current state. Stream ciphers represent a line of cipher development, which is different from block ciphers although there are simple mathematical transformations that convert stream ciphers to block ciphers and vice versa. They are generally faster to execute in hardware than block ciphers.

Symmetric cryptography:
Symmetric cryptography: Cryptography in which the same key is used for encryption and decryption.

Data encryption uses a session's key, which only lasts for the duration of the connection.

Asymmetric cryptography
Asymmetric cryptography: Encryption software that requires two keys: a public key and a private key. Encryption software users distribute their public key, but keep their private key to themselves. When someone wants to send an encrypted message, the sender uses the recipient's public key to encrypt the message, which can only be decrypted by the person who holds the corresponding private key. For example, Eric makes public key A and private key A, and Dan makes public key B and private key B. Eric and Dan exchange their public keys. Once they have exchanged keys, Eric can send an encrypted message to Dan by using Dan's public key B to scramble the message. Dan uses his private key B to unscramble it. If Dan wants to send Eric an encrypted message, he uses Eric's public key A to scramble his message, which Eric can then unscramble with his private key A. Asymmetric cryptography is typically slower to execute electronically than symmetric cryptography but hence the manageability of keys distributions.

Asymmetric algorithm
RSA: developed by Ron Rivest, Adi Shamir and Leonard Adleman. It provides digital signatures, key distribution function, and encryption. Based on difficulty to factoring large numbers. Used with SSL and PGP.
Diffei-Hellman key: Old hybrid crypto based on two algorithms sym/asymmetric. For key distribution only. Vulnerable to man-in-the-middle attack.
El Gaamal: Provides signatures, encryption, and key exchange. Based on algorithm discrete calculation in a finite field.
Elliptic Curve Cryptosystem (ECC): It provides digital signatures, key distribution function, and encryption. More efficient and doesn't require a long key to provide higher protection.

Hybrid approach:
The hybrid approach uses both asymmetric and symmetric algorithms introducing a secure way to transmit symmetric keys. This method seals the weakness of both systems. The sender encrypts the message with a symmetric key, then the symmetric key is encrypted with the recipient's public key, finally the encrypted message + encrypted symmetric key is sent to recipient. The recipient decrypts in reverse order using is private key.

Key management:
Ensures that keys are generated and stored securely. Here are some key management issues: key length should be long enough to provide proper protection; keys should be stored and transmitted using a secure means; key's lifetime should match the info under its protection; back-up and escrow the keys; not in clear text; the amount of keys increases compromise; user training; one-key one-app; multiple control key recovery

Integrity and signatures(hashing)
To provide message integrity (no alteration) a one-way hash is calculated creating a fixed-length hash value or Message Digest. Sender puts message trough the hashing algorithm to get a MD, then both the MD + message are sent. The receiver recalculates the hash value like the sender and compares the two values. Various attacks can occur such as: collision (2 messages with same hash), birthday attacks (brute force). Hashing algorithms are MD2, MD4, MD5, HAVAL, SHA (160).

Message Authentication Code:
MAC is a keyed message digest meaning it is formed by the originators' key. MIC Message Integrity Code is a not key but rather an algorithm. MAC is a weak form of authentication, which uses hashing algorithm and symmetric key. It works the same as one-way hashing except that the key + message are hashed. If the message is modified then the MD is different.

Electronic signature: verifies the sender creating an MD, inputted in a digital signature algorithm (private key), MD encrypted with private (sender) key. Public key verifies the signature by recreating the MD with message only and decryption of sent MD. If both MD = same then verified. Signature is used for e-contracts, virus protection (integrity), digitizing a hand signature is not safe. Example of signature DSS, SHA.

Msg encrypted = confidentiality
Msg hashed = integrity
Msg signed = authenticity, integrity, non-repudiation.
Msg encrypted + signed = confidentiality, authenticity, integrity, non-repudiation.

Cryptography applications:

Mail application:
Privacy-enhanced Mail (PEM)
Message Security Protocols (MSP) same as PEM but military purposes.

Pretty Good Privacy (PGP). Is a cryptosystem that uses symmetric sessions keys for message encryption and uses asymmetric keys for signature, integrity and key exchange. It is a Freeware e-mail client software, where the users can use various algorithm for data encryption, hashing and signatures. PGP uses web of trust, where users trust each other.

S/MIME: A standard that extends the MIME (Multipurpose Internet Mail Extensions) specifications to support the signing and encryption of e-mail transmitted across the Internet.

Internet security applications:
S-HTTP: An encryption protocol used to allow private communication on the Web. Allows encryption, digital signatures, authentication, or any combination of these, at the application level. Contrast with SSL.
HTTPS: The Hypertext Transport Protocol (Secure), the standard encrypted communication mechanism on the World Wide Web. This is actually just HTTP over SSL.
SSL: Secure Socket Layer, industry standard method for protecting Web communications. SSL security protocol provides data encryption, server authentication, message integrity and optional client authentication for a TCP/IP connection. SSL comes in two strengths, 40-bit encryption and 128-bit.
SSH2: The Secure SHell. A cryptographically strong replacement for rlogin, telnet, ftp, and other programs. Protects against "spoofing", man in the middle attacks, and packet sniffing.
SET: Secure Electronic Transaction (layer 7) is a secure protocol designed by MasterCard and Visa to facilitate financial transactions over the Internet. Unlike SSL, it stresses validating both parties to the transaction, and uses trusted servers so that a merchant holds only transaction identifiers, not actual credit card numbers.
IPSec: IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices.

Public Key Infrastructure
PKI is a framework that generates a public/private key pairs and exchange them. Ensures authentication, confidence, non-repudiation, and integrity using hybrid approach. The components are:
Certification Authority (CA) issues certificates, signs certificate(private key), trusted, public > internet, private > org; *certificates,* secure means of distributing public keys, associates public keys to owner, signed.
Know the following: receiving certificates, CA hierarchy, Cross-certification.

[1] Although the Official guide to CISSP exam edition 2004 at page 426 says that the message digest is 160bit, the RFC1321 says it has 128bit.

Registration Authority: accepts and verifies registrations info, accepts and authorizes requests certificates revocations, can't issue cert. Offload load from CA.

Certificate revocation list CRL: the CA responsible for creating, giving, and revoking cert. However the CRL manages the list. Signed data with time stamp, list revoke cert., user verify from CRL cert.
PKI steps: 1) sender asks the public directory for the receiver's public key. 2) Directory sends the key. 3) Sender generates a session key, encrypts it with receiver public key then sends it. 4) Receiver requests and validates sender public key from the public directory. 5) They trust each other and encrypt their message.

One-time pad: it is a large, many variable length bits, which is used to encrypt/decrypt a message. Once the session is completed the key is destroyed. The receiver must use the exact same pad to decrypt. One-time pad operates as stream ciphers

Attacks:
Cipher-only attack: when an attacker gets the cipher text of one or more message. By looking at the pattern of several messages the attack can guess the key.

Known-plain text attacks: reverse engineering the plaintext with known cipher text to get the key.

Chosen-plaintext attack: the attacker chooses the plaintext that gets encrypted. In this type of attacks the plaintext is sent to get and gets encrypted, as a result both the plain and encrypted are available. Probabilities are assigned to each key until the most likely key is found.

Name	Purpose	Type	Block size	Rounds	Key size	Remarks
DES data Encryption standard	Secrecy	Block cipher symmetric	64 bits not variable	16	56 + 8	Built in 74 by NIST. Uses MAC for integrity and authentication. Comes in different modes: ECB, CBC, CFB.
Triple DES	Secrecy	Block cipher symmetric	not variable	48		Modes: DES-EEE3, DES-EDE3, DES-EEE2, DES-EDE2. Uses 2 or 3 separate and different key.
AES Advanced Encryption Standard	Secrecy	Block Symmetric	128	10 - 14	128, 192, 256	Hardest of the commercial to crack
IDEA	Secrecy	Block Symmetric	64	8	128	Used in PGP
RC5	Secrecy	Block Symmetric	32, 64, 128 variable	255	0 - 2048	RSA
RC6	Secrecy	Block Symmetric	32, 64, 128 variable	0 - 255	0 - 2048	The difference with RC5 is it uses 4bit register vice 2 and makes it faster.
Twofish	Secrecy	Block Symmetric	128	16	256	
Blowfish	Secrecy	Block Symmetric	64	16	448	Schneier
RSA	Secrecy & signature	Asymmetric			768, 1024	based on the difficulty of factoring large numbers
ECC (elliptic Curve)		Asymmetric				
DSA	Signature	Asymmetric			512 - 1024	
Diffie-Hellman	Key exchange	Asymmetric			768, 1024	
El-Gamal	Secrecy & signature	Asymmetric			768, 1024	base on calculating discrete logarithms
SHA-1	Integrity	One-way	512		160 bit digest	
MD5	Integrity	One-way	512	4	160 bit digest[1]	

Adaptive chosen-plaintext: the attacker picks the plaintext to encrypt dynamically. The results of cipher text alter the attacker choice of the next plain text.

Chosen-cipher text: similar to chosen-plain text, but attacker picks the cipher text to be decrypted and has access to the resulting decrypted plaintext.

Adaptive chosen-cipher text: attacker has free use of the actual decryption hardware, but does not have the proper procedures to extract the decryption key from it.

Man-in-the-middle: An active attack that typically is gaining information by sniffing or tapping a line between two unsuspecting parties. Then, receiving data from one party and sending it to the other party.

Algebraic attack: A method of cryptanalytic attack used against block ciphers that exhibit a significant amount of mathematical structure.

Analytic: **Key length** is an important issue in cryptography. Most cryptographic schemes are based on publicly known algorithms, so the problem of guessing the key is related to the mathematical security of the system, if no known 'structural weakness' in the algorithm exists. A key should be large enough that a "brute force" attack is infeasible.

Domain 6 – Security Models & Architectures

The purpose of access control is to protect information models and architectural network methods from unauthorized disclosure, modifications, and destruction. The main types of mechanism are physical administrative and technical.

Definitions:
Primary Storage is a temporary storage area for data entering and leaving the CPU
Random Access Memory (RAM) is a temporary holding place for data used by the operating systems. It is volatile; meaning if it is turned off the data will be lost. Two types of RAM are dynamic and static. **Dynamic RAM** needs to be refreshed from time to time or the data will be lost. **Static RAM** does not need to be refreshed.
Read-Only Memory (ROM) is non-volatile, which means when a computer is turned off the data is not lost, for the most part ROM cannot be altered. ROM is sometimes referred to as firmware.
*Erasable and Programmable Read-Only Memory (EPROM***)** is non-volatile like ROM, however EPROM can be altered.
Process states: Stopped, waiting, running, ready
Cooperative computing is when
Preemptive computing

Computing principles
The *arithmetic logic unit (ALU)*, which performs arithmetic and logical operations.
The *control unit*, which extracts instructions from memory, decodes and executes them, calls on the ALU when necessary. Threads are part of a process that can execute independently of other parts.

The ability to execute more than one *task* at the same time is called multitasking. The terms *multitasking* and *multiprocessing* are often used interchangeably, although multiprocessing implies that more than one CPU is involved. The ability of an operating system to execute different parts of a program simultaneously is called *threading.*

Operating system mechanism
Virtual memory: It combines the computers' main memory to the secondary storage to make it looks like as one. When the main memory is filled the memory manager starts filling the swap space on the hard-drive "swapping". When an application calls for the data on the swap space it pages the memory to the main memory. The memory manager keeps a page table to track the frames and is located between the application and the main memory. Each page is 4 to 8 Kbytes segments.

Operating states: the computer works in different security modes depending on the classification and clearance. A *single state machine* operates in the security environment at the highest level of classification of the information within the computer. In other words, all users on that system must have clearance to access the info on that system. On the other hand a *multi-state machine*

can offer several security level without risk of compromising the system's integrity.

Security modes of operation: there two modes; one is the *dedicated security mode* where all users have the same clearance and need-to-know to read to information. The other one is c*ompartmented security mode* where all users have the clearance but not have the need-to-know.

Protection rings:
Ring 0 - Operating system kernel. The OS' core. The kernel manages the hardware (for example, processor cycles and memory) and supplies fundamental services that the hardware does not provide.
Ring 1 - Remaining parts of the operating system
Ring 2 - I/O drivers and utilities
Ring 3 - Applications and programs

Security models
Bell-LaPadula: model based on the *simple security rule* which a subject cannot read data at a higher security level (no-read up) and *security rule* which a subject cannot write information to a lower security level(No write down or *). This model enforces the confidentiality. Used by military and government organization.

Biba: Similar to Bell-LaPadula but enforces the *integrity star property* (no write up) and the *simple integrity property* (no read down). This model prevents data from other integrity levels to interact. Used by mostly by commercial organizations.

Clark-Wilson: A model that protects integrity, which requires a subject to access data through an application thus separating duties. This model prevents unauthorized users to modify data; it maintains internal/external reliability and prevents authorized users to wrongly modify data.

State Machine: The model from which the Bell-LaPadula and the Biba are derived, it protects itself from any activity that occurs in the system including *state transition*. It determines what resource a subjects can or cannot access.

Information flow: It focuses on object security policy to control resources (ACL) to allow or restrict access to object from subject. The information flows in the way the policy dictates it.

Non-interference: multi-level system (secret, confidential…) the system provides different level through domains and each domains or environment dictates what the users can access. Each domain does not affect another domain.

Brewer and Nash: The Chinese model provides a dynamic access control depending on user's previous actions. This model prevents conflict of interests from members of the same organization to look at information that creates a conflict of another members of that organization. Ex. Lawyers in a law firm with client oppositional.

Graham-Denning: This model is based on a specific commands that a user can execute to an object.

Harrison-Ruzzu-Ullman: This model is the same as above but it defines how access rights can be changed.

Security evaluation types

Trusted Computer System Evaluation Criteria
TCSEC: (Orange) From the U.S. DoD, it evaluates operating systems, application and systems. It doesn't touch the network part. It gauges the customer as to what their system is rated and provides a set of criteria for the manufacturer guidelines to follow when building a system. The break down is:

- D – minimal protection, any systems that fails higher levels.
- C1, C2 – Discretionary security protection. (1) Discretionary protection (identification, authentication, resource protection). (2) Controlled access protection (object reuse, protect audit trail).
- B1, B2, B3 – Mandatory protection (security labels) based on Bell-LaPadula security model. (1)Labeled security (process isolation, devices labels). (2) Structured protection (trusted path, covert channel analysis), (3) security domain (trusted recovery, Monitor event and notification).
- A1 – verified protection/design.

Rainbow series: Red (network), brown (trusted facilities management), tan (audit), aqua (glossary).

Information Technology Security Evaluation Criteria
ITSEC: it is used in Europe only, not USA. Unlike TCSEC it evaluates functionality and assurance separately. Assurance from E0 to E6 (highest) and F1 to F10 (highest). Therefore a system can provide low assurance and high functionality or vice-versa.

Functional requirements: identification/authentication, audit, resource utilization, trusted paths/channels, user data protection, security management, TOE access, communications, privacy, cryptographic support.

- F1 – F5 mirror functionality
- F6 required for system with high integrity i.e DBs
- F7 high availability on system
- F8 high confidentiality on system
- F9 high integrity on communications
- F10 high demand on integrity and confidence during communications

Assurance requirements: guidance document, configuration management, vulnerability assessment, delivery and operation, life cycle support, assurance maintenance, development, and testing.

- E0 inadequate assurance assigned to failed E1
- E1 informal design
- E2 informal design, testing, config control,
- E3 testing evidence of security mechanism
- E4 formal policy, semiformal spec on function architec
- E5 close correspondence between source & design
- E6 formal spec of architectures, formal policy

Common Criteria
Common criteria is an international standard to evaluate trust. TCSEC having a too rigid security and ITSEC having loose security criteria, the ISO produced the common criteria evaluation. It is a combination of TCSEC, ITSEC, CTCPEC, and the federal criteria. It defines two sets of requirements, functional and assurance then combines them in one rating; the Evaluation Assurance Levels (EAL) 1 to 7 level.

Evaluation Assurance Level
EAL 1 – functionally tested,
EAL 2 – structurally tested.
EAL 3 – methodically tested and checked,
EAL 5 – semi formally designed and tested,
EAL 6 – semi formally verified design and tested,
EAL 7 – formally verified design and tested.

CS-1 equivalent to TCSEC C2
CS-2 separation of duty, usage of ACL, strong password, availability, enhance security, audit mechanisms.
CS-3 Role-based control, non-discretionary control, strong authentication, administration and assurance.

Certification Vs Accreditation:
The *certification* is the technical procedures that render the accreditation. It uses safeguard evaluation, risk analysis, verification, and testing auditing techniques to assess the system suitability to the security level. The *accreditation* is a formal process to approve the system. The certification is presented to higher management and is then approved by them.

Domain 7 – Operation security

Operation security is keeping the organization system running securely. It is important to secure the day-to-day operation.

There are three types of personnel involved in operations.
Operator: monitors, executes system, controls job flow, mounting/volumes, initials program load, renames and labels resources, reassigns ports and lines.
Network administrator: maintains and controls network operation, and administers all device system tasks.
Security administrator: implements user clearance, sets up user profiles, configures level of sensitivity, reviews audit logs, implements communication security.

Definitions:
Production library: set of software used during operation.
Programmer library: set of software being developed.
Degaussing: the process of demagnetizing a magnetic material such that its remnant magnetism is zero
Zeroization: sanitization method by erasing electronic data and altering the content so that it cannot be recovered.
Sanitize: to expunge data from storage media (e.g., diskettes, CD-ROMs, tapes) so that data recovery is impossible using degaussing, physical destruction or overwriting
Overwriting: the technical process by which all addressable locations on a storage medium are filled with random data. Some software write zeros and ones (0/1).
Striping: storage method in which a unit of data is distributed and stored across several hard disks, which improves access speed but does not provide redundancy.
Mirroring: storage method in which data from one disk is duplicated on another disk so that both drives contain the same information, thus providing data redundancy.
Interleave: occurs when a drive is set up so that its sectors are not consecutive. Interleaves other than 1:1 were used by older interfaces or drives that could not handle fast seek times.
Hamming code:
Parity: Data integrity checking that adds a single bit to each byte of data. The parity bit is used to detect errors in the other 8 bits.
Clustering: Linking many small computers to do a big job.
Social engineering: Gaining information needed to access computers by means of tricking company employees by posing as a magazine journalist, telephone company employee, or forgetful co-worker in order to persuade honest employees to reveal passwords and other information.

Operation controls
Many operational resources must be protected: sensitive data, source code, hardware, password files, system utilities, audit logs, back-ups, and storage media. To protect them, operational controls must be in place: access to physical system, media, and separation of duties.

Separation of duties is a good administrative control that ensures that one person alone cannot compromise the organization security in any way. High-risk activities should be separated to more than one personnel. *Job rotation* is when more than one person fulfills the tasks of one position and therefore more employees understand the duties of the job. Also job rotation can lead to the discovery of fraudulent activities. *Mandatory vacation* acts the same as job rotation. *Need-to-know* only those people that must know about typical information have access to that information. *The least privileged* this means individual should only have enough access right to do their job, no more. *Clipping level* it is the baseline or the threshold when violating activities sounds the alarm. Usually an IDS is used as the watchdog for the clipping level. The clipping is done to find bad activities before they get really bad.

Here are some control categories: corrective, deterrents, recovery, compensation, preventive-administrative, preventive-physical, preventive-technical, detective-administrative, detective-technical, and detective-physical.

Configuration management and media control:
The configuration management is to identify, control, account for auditing changes to the baseline. All of this, for system stability. Some examples of changes are: new computer and applications, change in configuration, patch update, new technology, update policies, and new network devices…

One of the most important resources to protect is the media library. It holds software and data for and about the company, and it is basically the back-ups. Some of the methods to destroy media are overwriting, degaussing, and physical destruction.

Reacting to failures and recovering:
Trusted recovery is a protection against possible security bypass during failure or recovery. A *system reboot* is proper shutdown and restart. It can happen because of critical tables, system object data structures or lack of physical space. The release of the resources brings a more stable system. *Emergency system restart* takes effect after a system failure happens in an uncontrolled manner. *Cold start* unexpected TCB and the regular recovery system cannot bring system files to a reliable condition.

Systems can react in four different ways:
Fail-safe is automatic termination and protection of system to protect system environment.
Fail-soft termination of non-essential processes, most processes are still kept running.
Fail-secure keeps the system secure during and after failure. No matter what processes need to be shutdown the system will keep the system protected.
Fail-over occurs when a back up is activated taking over processing.

When a crash occur: boot into single-user mode (UNIX) Safe-mode (Windows), uninstall process/program disrupting, recover files, restore missing files, check integrity/security of files, then boot to regular mode.

Availability:
In order for an organization to function properly the information must be available when required. To make the info available the administrator should implement redundancy and effective back-ups.

Redundancy Array of Inexpensive Disk (RAID) are fault tolerant providing separation between HD units and redundancy.

RAID level table

Level	Characteristics	Availability techniques
0	Stripped, no redundancy, interconnected disk, high performance	Stripping
1	Mirrored, redundant	Mirroring
2	Striped at bit level, use up to 32hd storage + 7hd error recovery, no used	Hamming code parity
3	Striped, parity data on one hd at byte level, hd reconstruction from parity	Byte-level
4	Striped, parity data on one hd at block level, hd reconstruction from parity	Block-level
5	Data and parity are shared on the same hd, no single point failure	Interleave
6	Same as 5 but has a second set of parity data written	Double parity
10	Data is striped and mirrored across several drives, can support drive failures.	Striping & mirroring

Most used RAIDs are 1,3,5

Other availability mechanism is to have redundant servers and server clustering which is using a server farm as one unit but in different box. Clustering: is a series of redundant disks logically connected, which improves availability and scalability.

A backup is the process of copying files (copying) or bits (imaging) to a safe place in case of corruption or loss of the original files. Backup provides availability to resources. To perform a backup the critical data must be identified, schedule must be outlined, backup type (full, incremental, differential, on-demand), where to store.

Fax security:
Facsimiles represent certain important security problems. When transmitting sensitive information the link is usually in clear; fax does not encrypt. Unattended fax can offer attackers the ability gain access to unattended received fax. To alleviate the issue fax server can be used to reroute incoming faxes to a user's mailbox. However, it does not prevent fax sniffing in between the line the two-component originator/recipient. Therefore, bulk encryption methods must be used. *Bulk encryption* encrypts every bit going to the line.

Domain 8 – DRP & BCP

Disaster Recovery Plan (DRP) contains procedures to reduces damage during and after a tragic event. Business Continuity Plan (BCP) is a long-term plan to keep business functional following a disaster.

BCP: employees training on critical business functions; reducing business interruption; restores from backups to return to normal operations.
The DRP includes: Showing employees how to respond to disasters; developing emergency responses procedures; reducing impact of immediate dangers; restoring critical IT systems.

Definitions:
Incremental back up: backup level in which only files that have changed since the last backup are backed up of any sort.
Differential back up: back up level in which only files that have changed since the last full backup are backed up.
Full back up: backs up all files, modified or not; and removes all archives flags.
Disk shadowing: uses two physical disks where the data is written to both drives alike as redundancy purposes.
Electronic vaulting: the transfer of backed up files to a remote site using communications lines.
Remote journaling: activity of saving data in two locations, one on site, the other off site, simultaneously.
Hot site facilities: An emergency alternate site with a duplicate IS already set up and running, maintained by an organization or its contractor to ensure continuity of service for critical systems in the event of a disaster. Ready within hours
Warm site facilities: same as hot site but no computers just peripherals.
Cold site: An alternate site with necessary electrical and communications connections and computer equipment, but no running system, maintained by an organization to facilitate prompt resumption of service after a disaster.
Rolling hot site: it is a hot site on wheels.
Redundant site: provides an exact duplication of the operational site ready to go. More expensive than other site types.
Mean Time To Repair (MTTR): is the amount of time to get a device back into production.
Mean Time Between Failure (MTBF) is the expected lifetime of device, calculates risk of utility failure, and a metric used to compare devices.
SLA Service Level agreement

Possible threats:
To sort the possible threats they are divided in three main categories:
Non-disaster/incident: a disruption as result of a device or software malfunction. Solution: file and device restoration.
Disaster: the facility is unusable for a day or more. Solution: use of other site temporally while fixing equipment.
Catastrophe: destruction of the whole facility. Solution: use off-site facility for immediate operation. Long-term rebuild.

Steps in preparing the BCP
1. Project initiation
Management support, establish need for a plan, define scope and objectives, establish team representatives, identify responsibility, schedule meeting, determine the need for automated data, collection tools, and present initial report to management.

Duties of senior executives:
Support and drive the plans, ensure testing is carried out, oversee budget and funding needs.

Duties of functional management:
Identify and prioritize mission-critical systems, and monitor plan progress

Recovery and continuity committee:
Have various department members coordinate to all departments, develop analysis group, and outline the project schedule.

2. Business impact analysis (BIA):
Performed at the beginning of the disaster and recovery planning. It is an analysis that identifies all possible threat qualifying and quantifying the effect on the company overall service level.

Eight steps of BIA: 1) Select interviewees collecting data. 2) Determine how to gather data. 3) Qualitative and quantitative question package. 4) Analyze gathered data. 5) Determine time-critical function. 6) Calculate MTD for each function. 7) Prioritize MTD assets. 8) Document and present findings to executives.

a. The BIA identifies critical business functions like: IT net support; data processing; accounting; payroll; customer support; marketing/transaction devices; production scheduling; and more. Because of the interdependencies of each department, the analysis must focus on those issues.

b. Once the threat and critical business function identified, specific loss criteria must be identified like: loss of profits, loss of competitive advantage, increase in operation expenses, loss of revenue, loss of productivity, loss of customer satisfaction; and more. Losses can directly affect or indirectly affect the company.

c. It calculates the Maximum Tolerable Downtime (MTD) that the company can survive without it (depends of the tolerance of the business)

Non-essential = 30 days
Normal = 7 days
Important = 72 hrs
Urgent = 24 hrs
Critical = minutes to hours

3. Recovery strategies/plan
The purpose of a recovery plan is to improve responsiveness, ease confusion, and help decision making during a crisis. The DRP must regard certain key information: *responsibility*, everyone responsibility should be outlined, all tasks should be assigned to each individual; each individual should know what is expected of them during a crisis. *Authority:* during crisis know who is in charge to give proper directive. *Priorities*: very important to know what is critical Vs nice-to-have. Which devices, system or function must be up and operational first. *Implementation and testing*: the plan must be implemented and tested.

Incident Response Plan (RP) is a document that explains how to react before it happens. It lists outside agency, computer/forensic experts, how to preserve evidence, search for evidence, report procedures, outline who (*incident response team*) does what in case of an attack. The executive must be aware of the attack and investigation.

Recovery and restoration: this process should be done by two teams, one to get the alternate up and running, the other restoring the old destroyed site.

Emergency response plan should be practiced regularly to minimize confusion and life threatening situations.
The DRP should include the following documentation: facilities issues; people; hardware; software; supplies; recovery procedures; emergency procedures; external contact.

Back-ups and off-site facilities
Backup issues:
Do we have backups of OS and software;
System config documented and off-site;
Have redundant connection to remote sites;
How quickly can we get replacement equipment;
Are there interoperability issues for replacement equipment;
Do we have backup of configuration for all devices;

Storage issues:
Time frame to access back-ups;
Open state of storage facilities, is open on weekends;
Is access secure, alarm devices against robbery or fire;
Availably of bounded transport systems;
Any hazards like flood, tornados, hurricanes…
Does the facility have proper climate control;

4. Plan design and implementation
Written documents that record the results of the BIA and document in details the recovery plan.

5. Testing, maintenance and awareness training.
Test and drills: has the main goal of confirming the plan works. The test should be regularly done; the test should address all weaknesses of the plan and rectify them. Example of test:
Checklist test: the DRP and BCP are distributed to all departments. Then all dep. mention any problems to the master plan.
Structured walk-through test: all members meet to discuss and brainstorm the plan.
Simulation test: all employees practice a disaster recovery.
Parallel test: the alternate site is put in function. The two sites works at the same time and the two sites' output is compared.
Full interruption test: the actual site is shut down and tested. This test has more impact on the main function of the business.

Maintenance plan: can quickly fall out of date because company re-org, personnel turnover, environmental change, hard/software change, plan just not looked after. Here are methods to ensure the plan gets the proper updating: integrating it into job description, include the BCP in the personnel evaluation report, conduct regular audits, regular report or meetings, use timed software to alert when to look at it.

Domain 9 – Law and ethics

Definitions:
Hacker: A clever computer programmer, who does not necessarily engage in illegal activities. 2) In the media, a hacker refers to a person who illegally breaks in or attempts to break into a computer system.
Cracker: A cracker is an individual who attempts to access computer systems without authorization. These people are often malicious, as opposed to hackers, and have many means at their disposal for breaking into a system.
Motivation: The relative amount of incentive that a threat has to compromise or damage the assets of an organization.
Opportunity: is a situation in which it is possible for a hacker to attack.
Means: is a method instrument, process to attack.
Downstream liability: Effect that a company may have toward a partner organization.
Legally recognized obligation: an expected standard of conduct to protect other company from unreasonable risks.
Proximate causation: a proof that the plaintiff incurs damages.
Evidence: Documents, testimony of parties or witnesses, or other objects of proof presented to the court. Types of evidence: best, secondary, direct, conclusive. Corroborative, circumstantial, opinion and hearsay.
Evidence direct is a type of evidence that is oral, witness
Evidence real is a tangible object to prove
Evidence physical is an actual object used in crime scene
Evidence documentary record or document computer
Evidence hearsay is second-hand evidence such computer tape, hard disk does not constitute allowable evidence in court.
Forensics: The science and practice of examining physical evidence and applying the physical properties of that evidence to the resolution of legal issues, particularly identifying the commission, nature, and perpetrators of crimes.
Chain of custody: An unbroken trail of accountability that ensures proper keeping of the physical security of samples, data, and records.
Enticement: something that seduces or has the quality to seduce. Honey pots.
Entrapment: The illegal tricking act of inducing a person to commit a crime so that a criminal charge will be brought.
Honey pots: A host or network with known vulnerabilities deliberately exposed to a public network. Honey pots are useful in studying attackers' behaviour and also in drawing attention away from other potential targets.
Padded cells complement IDSs and are simulated environments to which IDSs seamlessly transfer detected attackers and are designed to convince an attacker that the attack is going accordingly.

Ethics institution
ISC2 http://www.isc2.org: is a global, non lucrative organization dedicated to maintain the Common Body of Knowledge for Information Security, governing body for ISSec ethics in CISSP. Visit their site for ethics before testing.

Computer Ethics Institutes www.cpsr.net: Computer Professional for Social Responsibility (CPSR); CPSR is a non-profit org which is concerned of the impact of information and communications technology on society.

Internet Activities Board www.iab.ie: IAB looked at issues surrounding the illegal and harmful Internet use; such as: child pornography, computer privacy, destruction of information integrity and more…

Hacker issues
Hackers have *motivation*, who and why for the attack. Most of the motivation is just a thrill to enter a forbidden zone or challenge to do so. However, when the hacker actually manipulates file, folder, or configuration to get a personal gain he/she is a more serious, dangerous hacker. *Opportunity* is the where and when of the hacking strikes. The *means* is how perpetrators entered the system.

The kinds of factors that attract hackers are companies with a lack of protection, slow response organization, no enforcement, and attractive information.

It is very difficult to get to the end prosecution of a hacker because of the lack of understanding the info, law, new crimes comes forward, difficulty to gather clues and proof, suitable punishment tough to judge, not always viewed as a major crime.

Establishing liabilities and ramification
Company can be proven guilty if not conducting business with due care and due negligence. There usually must be *legally recognized obligation* and there must *proximate causation.*

Privacy Act of 1974 (USA). Deals with data/information held by government agencies.
Electronic Communications Privacy Act of 1986 (USA). Extends the unlawful wiretapping to cover electronic communications.
Computer Fraud and Abuse Act 1986/96. The illegal use of federal computers.
Health Insurance Portability and Accounting Act (HIPAA) (USA). This act protects people's medical information.
Economic Espionage Act 1996 (USA). Provides structure to deal with espionage in the goal to get trade secrets.
Gramm Leach Bliley Act 1999 (USA). Requires that financial institution exert proper information security in training, risk management and develop security policies.

If a company desires to monitor its employees' activities, the company must somehow inform the employees of possible monitoring activities. It must be done lawfully, no employees can be singled out and only work-related actions can be monitored.

Trans-border information flow is the movement and storage of information across a border. It is important to know that there are legal issues to consider, certain countries deal differently with confidential, cryptographic type of information moved and stored.

Types of law
Criminal
Criminal law is a body of the law that deals with conduct considered so harmful to society as a whole that it is prohibited by statute, or common law, and is prosecuted and punished by the state.

Civil/tort
Civil law is the body of law relating to contracts and suits as contrasted with criminal law. Civil law covers suits of one party by another for such matters as breach of contract or negligence. The standard of proof in civil cases is preponderance of evidence - a greater weight of evidence exist, which is a weaker standard than absence of a reasonable doubt.

Administrative
Administrative law is rules and regulations that government agencies develop based on their interpretations of statutory law.

Intellectual property law
Trade secret
Trade secret is any confidential formula, pattern, process, device, information, or compilation of information that is used in a submitter's business, and that gives the submitter an opportunity to obtain an advantage over competitors who do not know//use it. The owner must exert due care.

Copyright©
Copyright is a legal right (usually of the author or composer or publisher of a work) to exclusive publication production, sale, and distribution of some work. What is protected by the copyright is the "expression" not the idea. Taking another's idea is plagiarism, so copyrights are not the equivalent of legal prohibition of plagiarism.

Trademark™
Trademark is a word, phrase, slogan, design or symbol used to identify goods and distinguish them from competitive products. Trademarks may be registered with the U.S. Patent and Trademark Office, and similar offices worldwide. However, in the US and in other countries with legal systems based on English common law, trademark rights also accrue through common law usage.

Patent
Patent is a document granting an inventor sole rights to an invention.

Investigating computer crime
Who does the investigation, internal staff, consultants or law enforcement? The main purpose of the investigation is to attempt to gather information to convict the attacker. Internal employees have limited amount of knowledge even if they have great knowledge of the organization. Consultants on the other hand have knowledge of security intricacy but are expensive, must be trusted, the info is controlled within the organization. Law enforcement is IT sec knowledgeable, information is not controlled, requires a search warrant. The management should be consulted to make the decision to have law enforcement (FBI/RCMP) intervene.

The CERT (Computer Emergency Response Team) must be careful in gathering the evidence of crime. Photograph the area before going in to the scene or systems, dump and preserve memory contents, power down, record the collection process and the *chain of custody*, get HR involved (disgruntled employees), send items to forensics.

During the forensics portion an image of disk must be made (not copying files, to preserves all bits), look for hidden files, viruses, slack spaces, fat table.

Before the evidence can be presented in court they must be competent, relevant and material.

Chain of custody
Once the evidence gathered, its accountability and integrity must be preserved to be admissible in court. It is to prevent tampering.

Evidence life cycle
It is a series of steps from the acquisition of the evidence until it is returned back to the owner. Throughout the process all the evidence must be carefully taken care of. The steps are:

- Collection and identification
- Analysis
- Storage, preservation, and transportation
- Presentation in court
- Return to owner

Types of attacks
Attacks are divided in three categories: physical, personnel, and operation.
Salami: insignificant or small procedure that produce a larger sum effect. It can also be divided in types: grudge, terrorists, financial, business, and fun.
Phone fraud: When you intentionally mislead another person or company to gain unjust free calls.

Domain 10 – Physical security

**** very important to check your local building codes**

Definitions:
Spike: momentary high voltage
Surge: prolonged high voltage
Fault: momentary power outage
Blackout: prolonged loss of power
Sag: momentary low voltage
Brownout: prolonged power supply below normal
Electromagnetic interference (EMI): electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a result of spurious emissions and responses,
Radio frequency interference (RFI): The unintentional or intentional transmission of radio signals. Computer equipment and wiring can both generate and receive RFI
Negative power: Actual loss of total power.
Surveillance: watching for unusual behaviour.
Detecting: sensing change into an environment

Fire class	Type of fire	Elements of fire	Suppression method
Class A	Common combustible	Wood, paper, cloth, certain plastics	Water, soda acid
Class B	Liquid	Petroleum, oils, solvents, alcohol, gases	$C0^2$, FM-200 (replacement for halon)
Class C	Electrical	Electrical equipment (computers)	Halon gases and $C0^2$
Class D	Combustible metals	Magnesium, sodium	Dry powder

Areas of physical security
Physical location:
When a company decides to inhabit a building several factor plays an important role. Hazards to be considered are natural disasters, local crime, access roads, tenants, air and road traffic, vandals and burglars, police, fire station, medical.

Construction:
When constructing a building facility attributes must be accounted for. Things like walls construction, ceilings, doors, HVAC, power supplies. Those attributes are fire rating, resistance to entry, alarms. Internal partition creating a barrier between two rooms should rise to the ceiling; most buildings don't offer this partitioning.

Computing area:
Should not be on the top floor, not in the basement, not on the first floor, not located next to stairs, bathroom or elevators, and should be located in the core of the building. These high security rooms should have no more than two doors, full-height walls, and all have one hour fire rating.

Electrical and environmental concerns
UPS: Uninterruptible Power Supply issues must consider the size of load, how long it can support a load, speed at which the UPS turns on, and physical space available. In UPS it is sought to have short battery life, remote diagnostic software, surge protectors.

To reduce negative power issue avoid fluorescent lights, use three prong plug, no daisy chains, do not put electrical data cable close to power source.

Power interference: Power interferences are due to either EMI or RFI across a power line. Ex. fluorescent lighting. To reduce power problems, noise, use voltage regulator, line conditioner, surge protectors, line monitors, UPS, shields long cable.

Environmental: Most electronics components must operate in a climate-controlled environment. A proper environment is; 20 - 23° C 68-72°F and 40 - 60 % hum. High humidity causes corrosion and low or dry air causes static electricity. To prevent electrostatic electricity use antistatic flooring, control environment, proper grounding, no carpet, use antistatic bands.

Ventilation (HVAC): creates positive air flow (positive barometric pressure in the area) so that when a door is open nothing gets in (uncontrolled, even the air gets restricted access) the room like contaminants dust, and smoke. During a fire HVAC can be automatically turned off.

Fire detection and suppression
Three components of fire are heat, oxygen, and fuel. If one of those are remove the chemical reaction of fire won't occur. Fire prevention is mandatory if the local fire building codes are followed in building construction, safety procedures, training, and housekeeping loss should be prevented. Main cause of a fire is electrical distributions. Many factors must be looked at when evaluating and estimating the occurrence rate of a possible fire, the amount of damage it can do to the information systems.

Detection
Detection: ionization detector (reacts to charged particle, early warnings), Thermal (fixed or rate-of-rise temp), photoelectric detector, infrared detector (reacts to heat of flames).

Suppression
Sprinklers system comes in various types. The *wet-pipe* where the pressurized water is kept and released, when detected only the specific sprinkler is activated. The *dry-pipe* system contains no water but pressurized air (good for below freezing room). The *deluge* system similar to wet-pipe but a whole area is watered. And the *pre-action* is the combination of wet-pipe and deluge. The water is released in two phases, first in a deluge to the areas then to each individual sprinkler.

Gaseous systems similar to dry-pipe use gases to extinguish fires. The gas can be:

- FM-200: similar to Halon, safe in occupied area
- Inergen: high-pressure gas composed of Nox, argon, CO2.
- CO2: dangerous to human
- FE-13 new and safest agent for human up-to 30% saturation similar to FM-200 and Inergen.

Halon is an ozone depleting gas that is banned in most area, and $C0^2$ is dangerous gas to breathing animals, but does not leave residue after usage. So $C0^2$ should be used such that it will not endanger people.

Perimeter security
Passage
Locks: Is the most inexpensive device to delay entry to persistent intruders. There are several lock types: *conventional locks* easily picked, key duplication; *pick-resistant*, more expensive; *electronic combination*, cipher or key-less; deadbolt, not part of door handle; smart locks certain person, specific times.

Cipher locks have different options; door delay, key-override, master keying, and hostage alarm.

Facility access: several methods exist to control access to an area: security guards, card, proximity card, which doesn't need to be swiped. There are two types of proximity cards - user activated and system sensing.

Piggybacking is when someone is using someone else's credentials. Tailgating is the physical following of someone to gain access.

A mantrap can protect entrance, which by using turnstiles or two doors to check credentials. An arresting/alarm system is used to stop the person.

Logs are a primarily use as detective devices than as preventive measures.

Fence
Fencing: not always attractive but very good at keeping bad guys out. Bollard are used approximately to parking and road, and are cement reinforced steel posts preventing vehicles ramming into buildings. Sometimes fences are used as deterrent therefore they are very visible like army bases and prisons. Others are hidden for cosmetic and marketing reasons. PIDAS Perimeter Intrusion and Detection Assessment System are devices that will be triggered when fencing is cut, touched. But can trigger lots of false alarms from natural forces.

Fencing characteristics:
3 – 4 feet high are deterrent only
6 – 7 feet high considered too high to climbed

Higher than 8 feet with barbed wire are serious protection and deterrent.

Lighting
Lighting: there are two reasons for having proper light. One is to provide proper illumination to employees at night to avoid court action and attacks on employees. The other is a deterrent to intruders. Lights for proper perimeter protection should (NIST) be eight feet in height and two feet out.
Surveillance devices:
One of the best surveillance devices is the security guard. It is especially good when discretionary judgment is needed. The best security plan doesn't rely on one system but several including guard dogs. Dogs are loyal, excellent sense of smell and sound perspicacious, and obey to commands well. CCTV allows recording activity and having peripheral vision controlled centrally.

IDS (physical):
List of Intrusion Detection System technology.
Proximity detection. Measure magnetic field variation
Photoelectric and photometric detects change in light with in an area. Good in closed rooms with no windows.
Wave pattern two components, a generator provides wave and receiver receives it. If the pattern is disrupted the alarms sounds

Passive infrared detects heat waves change within an area. Acoustical-semitic detection detects change in noises levels in the room. Must be used in a sound proof room.

Other detectors: contact, pressure mats, video motion, closed circuits, vibration, duress (tampering)

IDS issues: expensive, human intervention, requires redundant power supplies, should be fail-safe, should be tamper proof, they have lots of false alarms, penetrable.

OSI Model

***O**pen **S**ystem **I**nterconnection*, an ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

Layer name	Characteristics
Application (Layer 7)	This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.
Presentation (Layer 6)	This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the *syntax*.
Session (Layer 5)	This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.
Transport (Layer 4)	This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.
Network (Layer 3)	This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.
Data Link (Layer 2)	At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.
Physical (Layer 1)	This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

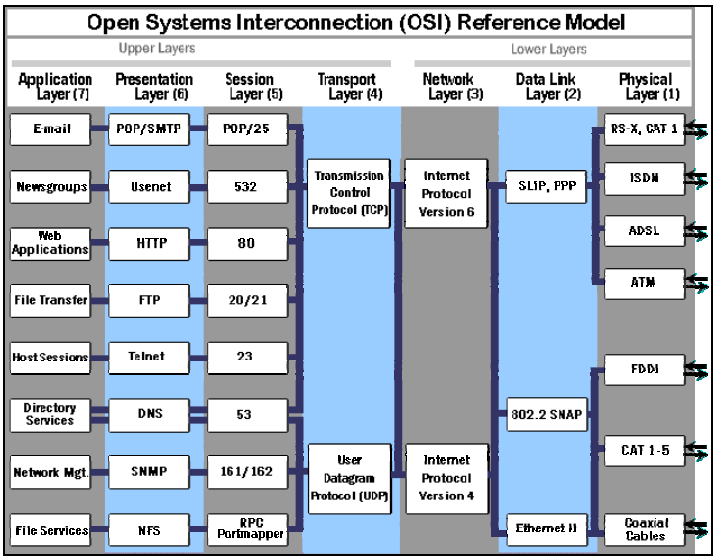


figure 1 (http://searchnetworking.techtarget.com)

TCP/IP *(Internet Reference Model)*

The acronyms TCP and IP stand for *Transmission Control Protocol* and *Internet Protocol*. *TCP/IP* was a grouping of two protocols. TCP/IP is a suite of networking protocols that provide much of the functionality of the OSI 7 layer model. However, the TCP/IP stack is somewhat more simple and is represented as four layers shown in the diagram below:

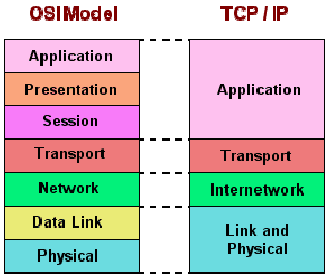


figure 2

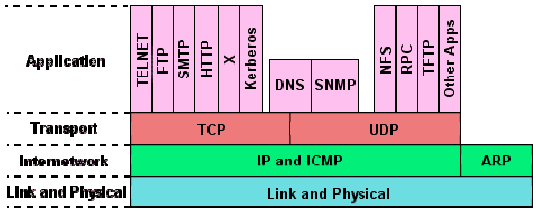


figure 3

Details of TCP/IP
The diagrams in figures 1 and 2 illustrate how these protocols are used in the stack.
In the diagrams applications depend on a preceding protocol. For example, FTP is encapsulated in TCP packets, not UDP.

Application layer
Telnet is an application allowing remote login to another computer providing a remote logon command-line access.
FTP (File Transfer Protocol). FTP allows users to upload files to, or download files from a remote computer.
SMTP (Simple Mail Transfer Protocol) it is the engine driving the transfer of email.

Transport layer
Within the TCP/IP stack, transport control is either handled by *TCP* - Transmission Control Protocol, or by *UDP* - User Datagram Protocol. The important difference is that TCP uses *virtual circuits*. I.e. connections between end-points are established, allowing data to flow reliably between them.
UDP, on the other hand, does not use pre-established circuits, and is thus termed a *connectionless* transport protocol. Since circuits do not need to be established in advance, UDP transport requires less network overhead and is therefore faster. For example, *TFTP* - Trivial File Transfer Protocol - uses UDP. TFTP is used to transfer config files. However, connectionless protocols are inherently unreliable. However, if the application itself implements some form of reliability checking, then UDP will clearly be preferable to TCP.

Internet layer
IP takes care of transporting UDP or TCP segments (packets) from start-point to end-point, based on their IP addresses.

ICMP (Internet Control Message Protocol) is used to request the status of network hardware, or to respond to such a request. For example, the *Ping* command uses an ICMP packet. ICMP reports routing failures, tests nodal reachability and increases routing efficiency.