Information/Cyber Security

Key Objective

- The protection of information and its critical elements, including the systems and hardware that create, use, store, transmit and delete that information.

- It is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

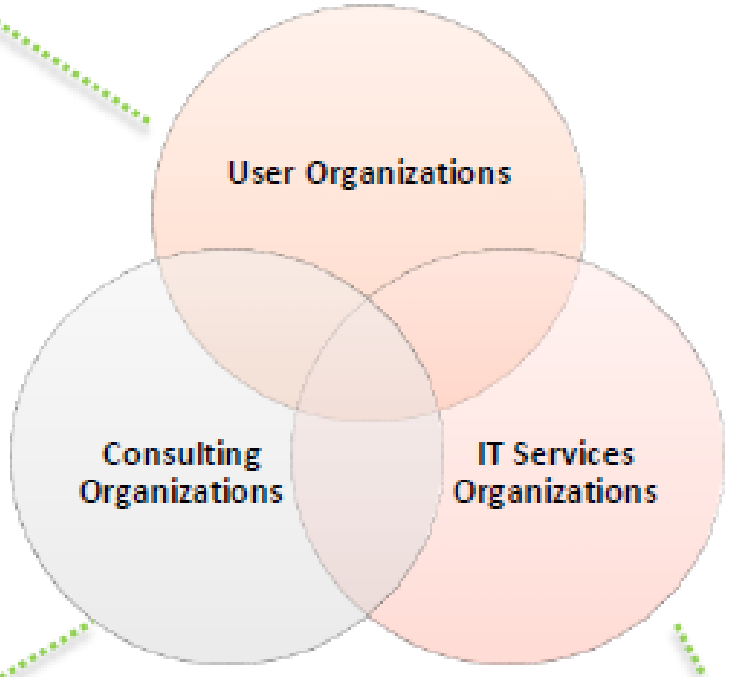
- It helps the organization’s mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.

Key Tracks


1. Network Security
2. Application Security
3. Data Protection and Privacy
4. Identity and Access Management
5. Cyber Assurance / GRC
6. IT Forensics
7. Incident Management
8. BCM/DR
9. End Point Security
10. Security Operations
11. Industrial Control Security

Figure : Types of organisations in Cyber Security, Source; IT-ITES Sector Skill Council NASSCOM

These organisations manages security of their infrastructure, applications and data They often use InfoSec services & products to safeguard their Cyber Security Assets. They could be from various other sectors like Banking, Healthcare, Telecom, Retail, IT-ITES, etc.
e.g CapGemini, Tata TeleServices, HSBC, Apollo Healthcare, etc.



InfoSec services firms help user organizations manage the aspects of their information security program by consulting, developing, implementing, administering, monitoring, maintaining and troubleshooting for InfoSec solutions.
e.g FIS, TCS, WIPRO, etc.

Consulting firms guide organizations in their strategies, initiatives and compliance with standards and regulatory requirements and also help them, ensuring protection of their network and critical IT assets, and that their staff is fully equipped to address external and internal threats.
e.g. Pwc, KPMG, Deloitte etc.

Information/Cyber Security Career Map

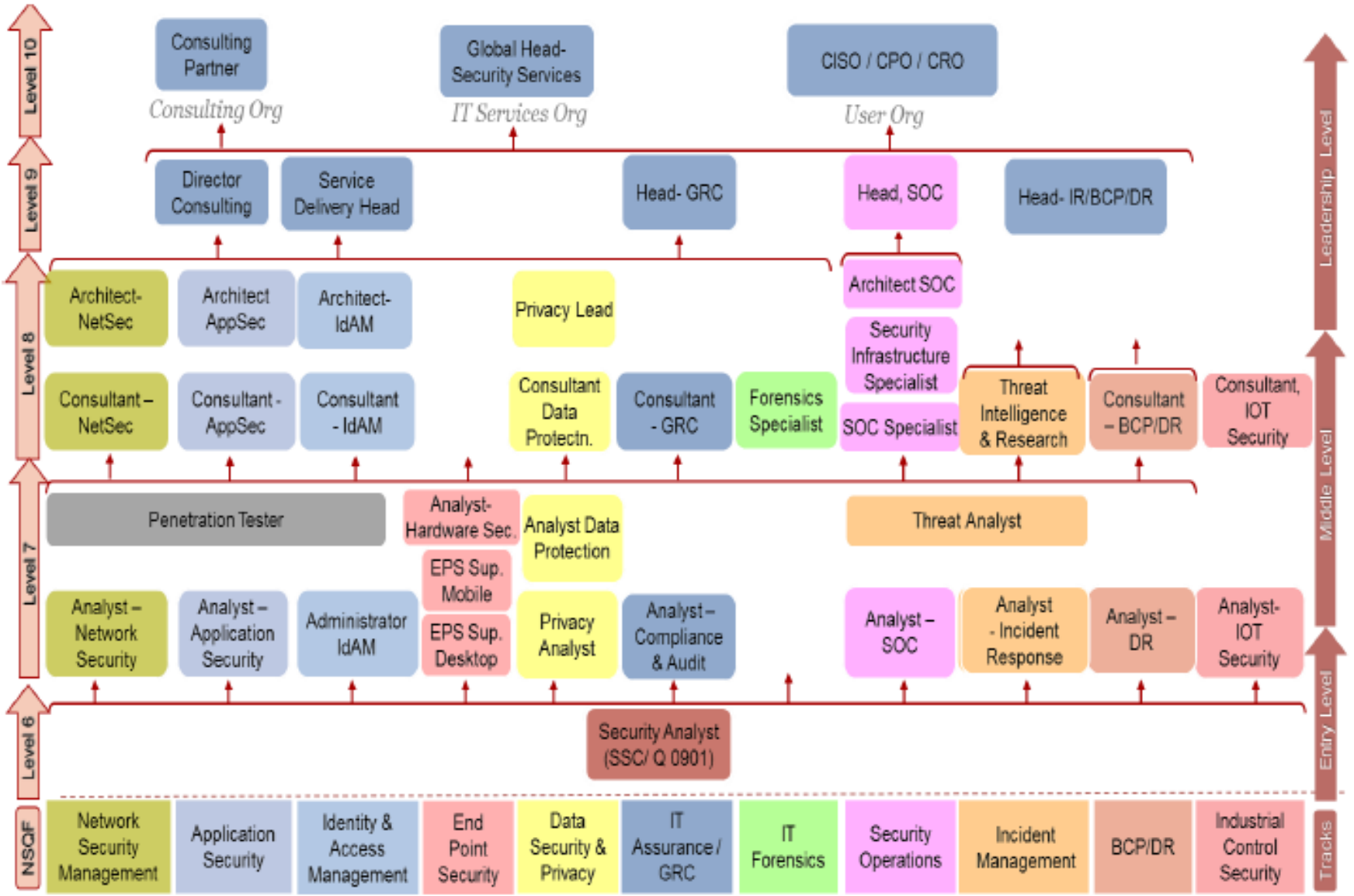


Figure : Information/Cyber Security Career Map, Source IT-ITES Sector Skill Council NASSCOM

1. Network Security

- to protect **networking components, connections, and contents from unauthorized access**, misuse, malfunction, modification, destruction, or improper disclosure.

2. Application Security

•to protect **various applications or the underlying system (vulnerabilities) from external threats** or flaws in the design, development, deployment, upgrade, or maintenance.

3. Data Protection and Privacy

•to prevent unauthorized access to **computers, databases and websites and protect data from corruption**. It also includes protective digital privacy measures.

4. Identity and Access Management

- •to enable the **right individuals to access the right resources** at the right times for the right reasons by authentication and authorisation of identities and access.

5. Cyber Assurance / GRC

•to develop and administer processes for **Governance, Risk and Compliance**

6. IT Forensics

•To **collect analyse and report on digital data** in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally.

7. Incident Management

- to manage information security incidents and **identify, analyze, and correct hazards** to prevent a future re-occurrence.

8. BCM/DR

•to develop and administer processes for creating systems of **prevention and recovery** to deal with potential threats to a company thus protecting an organization from the effects of significant negative events

9. End Point Security

•to protect the corporate network when accessed via remote devices such as **laptops or other wireless and mobile devices**. Each device with a remote connecting to the network creates a potential entry point for security threats.

10. Security Operations

- to monitor, assess and **defend enterprise information systems** (web sites, applications, databases, data centers and servers, networks, desktops, etc.)

11. Industrial Control Security

•to secure control systems used in industrial production, including **Supervisory Control And Data Acquisition** (SCADA) systems, **Distributed Control Systems** (DCS), and other smaller control system configurations such as **Programmable Logic Controllers** (PLC) often found in the industrial sectors and critical infrastructure

Security Operations Centre – An Introduction

- Information security is changing at a rapidly accelerating rate.

- Hackers are increasingly relentless, making the response to information security incidents an ever more complex challenge.

- Point solutions (**antivirus, IDS, IPS, patching and encryption**, etc.) remain a key control for combatting today's known attacks; however, they become less effective over time as hackers find new ways to circumvent controls.

Security Operations Centre – An Introduction

- A well-functioning Security Operations Center (SOC) can form the **heart of effective detection**.

- It can **enable information security functions** to respond faster, work more **collaboratively** and **share knowledge** more effectively.

- Organizations may **not be able to control** when information security incidents occur, but they can control how they **respond to them**.

Security Operations Centre

- A security operations center (SOC) is a **centralized unit** that deals with security issues on an **organizational and technical level**.

- A SOC within a **building or facility** is a central location from where a team primarily composed of security analysts are organized to **detect, analyze, respond to, report** on, and **prevent cyber security incidents**., using **data processing technology**.
-

SOC Services

- Provide a means for **reporting suspected** cyber security incidents
- Provide **incident handling assistance**
- **Disseminate** incident-related information to clients and external parties.
- SOCs can range from small (five-person operations) to very large (national coordination centers).

SOC's mission statement

1**. Prevention** of cyber security incidents through proactive:

a. Continuous threat analysis

b. Network and host scanning for vulnerabilities

c. Countermeasure deployment coordination

d. Security policy and architecture consulting.

2. **Monitoring, detection, and analysis** of potential intrusions in real time and through historical trending on security-relevant data sources.

3. **Response to confirmed incidents**, by coordinating resources and directing use of timely and appropriate countermeasures.

SOC’s mission statement

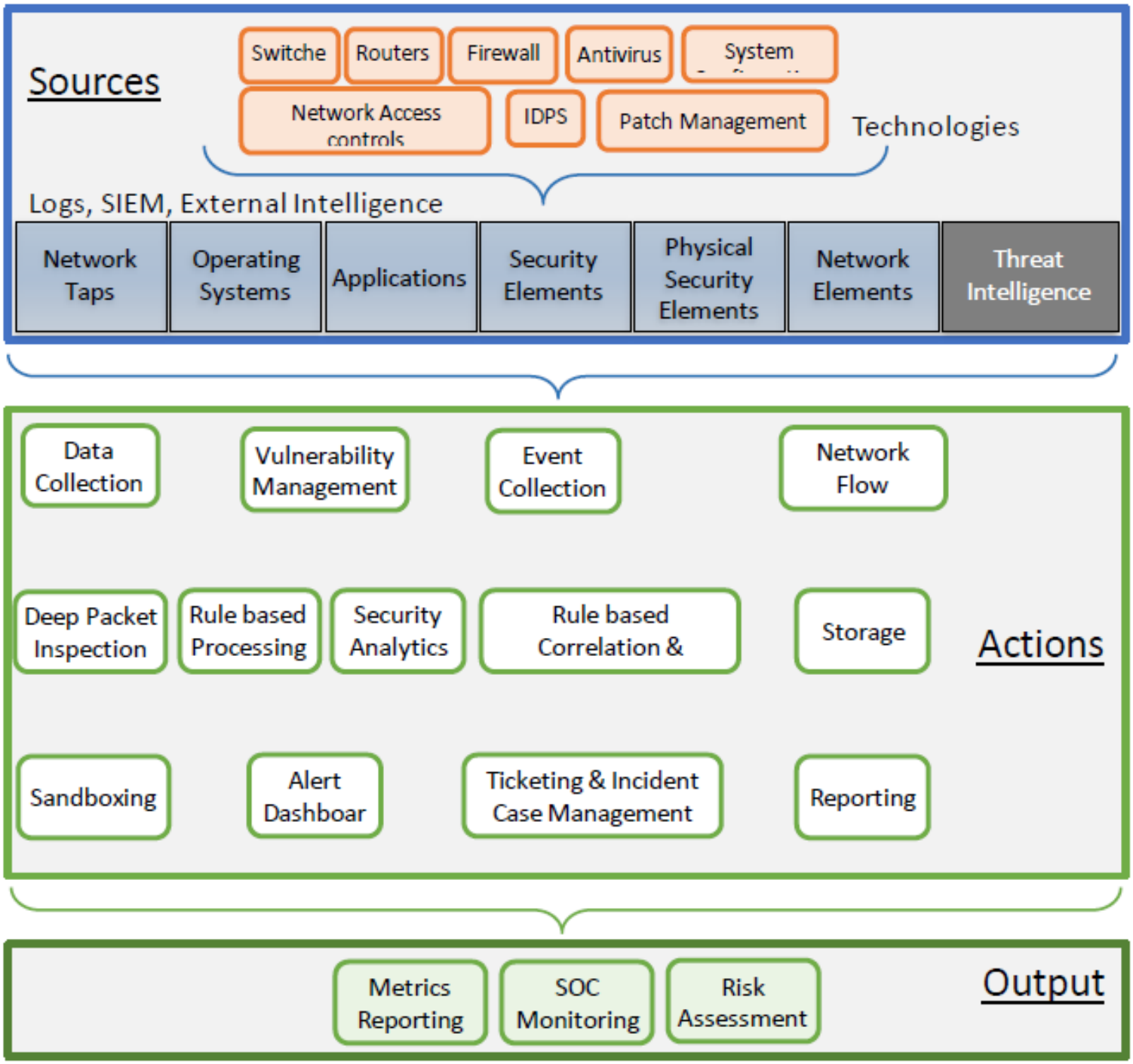
4. **Providing situational awareness and reporting** on cybersecurity status, incidents and trends in adversary behaviour to appropriate organizations.

5. **Engineering and operating CND technologies** such as IDSes and data collection/analysis systems.

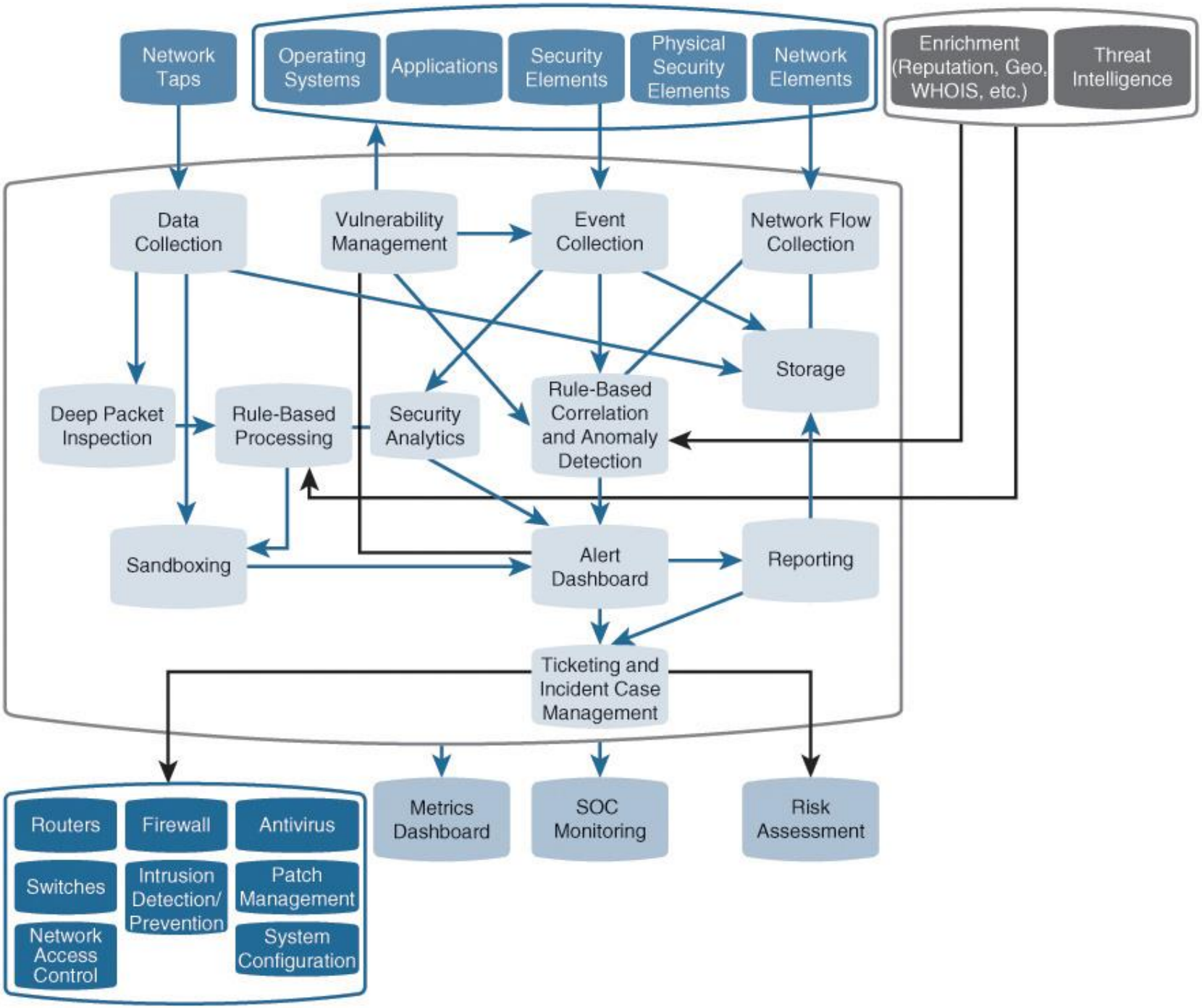
Analyst Security Operations Centre

- IDSes are systems placed on either the host or the network to detect potentially malicious or unwanted activity that warrants further attention by the SOC analyst.

- Combined with security audit logs and other data feeds, a typical SOC will collect, analyze, and store tens or hundreds of millions of security events every day.



Sample SOC Architecture


Network Taps
Operating Systems
Applications
Security Elements
Physical Security Elements
Network Elements
Enrichment (Reputation, Geo, WHOIS, etc.)
Threat Intelligence
Data Collection
Vulnerability Management
Event Collection
Network Flow Collection
Storage
Deep Packet Inspection
Rule-Based Processing
Security Analytics
Rule-Based Correlation and Anomaly Detection
Sandboxing
Alert Dashboard
Reporting
Ticketing and Incident Case Management
Routers
Firewall
Antivirus
Switches
Intrusion Detection/ Prevention
Patch Management
Network Access Control
System Configuration
Metrics Dashboard
SOC Monitoring
Risk Assessment

Security Operations Centers (SOCs) vs Network Operations Centers (NOCs)

- Both functions are frequently organized in a similar fashion using a tiered approach with similar roles at the lowest levels.
- They both share some tools, although each one also has a unique toolkit and techniques.
- Both groups leverage deep knowledge of the computing environment and require broad technical skills.
- NOC is primarily concerned with **serving the business**, the SOC's main focus is to **protect it**.

Security Operations Centers (SOCs) vs Network Operations Centers (NOCs)

- When an outage is detected, NOC personnel are likely to attribute the **disruption to device malfunction** or system issue and attempt to address it through hardware replacement or configuration adjustment.

- SOC personnel are likely to attribute the **problem to malicious activity** and will thus **prompt an investigation before initiating response actions**.

‘3 Level’ Structure of SOC

- **Level 1**
  - A SOC typically will designate a **set of individuals** devoted to **real-time sorting, categorizing, and prioritizing incoming events** and other requests for SOC resources, as well as **handling phone calls** from users and other routine tasks.
- **Level 2**
  - If Level 1 determines that an alert reaches some **predefined threshold**, a case is created and escalated to Level 2.
  - This threshold can be defined according to various types of potential “badness” (type of incident, targeted asset or information, impacted mission, etc.).
  - Level 1 members are discouraged from **performing in-depth analysis**, as they must not miss events that come across their real-time consoles.
  - If an event takes **longer than several minutes to evaluate**, it is escalated to Level 2.

Level 2

- Level 2 accepts cases from Level 1 **and performs in-depth analysis** to determine what actually happened—to the extent possible, **given available time and data**—and whether further action is necessary.
- Before this decision is made, it may **take weeks to collect** and **inspect all the necessary data** to determine the event's extent and severity.
- Because Level 2 is not responsible for real-time monitoring and is staffed with more experienced analysts, it is able to take the time to **fully analyze each activity set**, **gather additional information**, and **coordinate with constituents**.
- It is generally the responsibility of Level 2 (or above) to determine whether a potential incident occurred.

Level 3

- Level 3 is the advanced level and is primarily involved in **analysis, troubleshooting and resolution of complex technical problems** that impact Cyber security at the data, application, service, operating system and network levels. It is the **expert level**.

Organisational Structure of SOC

- SOCs are either **part of the organization** they serve or external to it.

- SOCs that are external to the organisation that they serve include **Managed Security Service Providers** (MSSPs) run by a corporation providing services to paying clients.

- Some examples are TCS, WIPRO, Infosys SOC teams.

- They also include SOCs that are **product focused**, such as those run by **vendors**, which must rapidly respond to security vulnerabilities in products that serve a large customer base.

Organisational Structure of SOC

- In most cases, a SOC is part of the organization it defends; therefore, its **relationship** is considered **internal**.

- An internal SOC's serves **a set of users and IT assets** that belong to one autonomous organization, such as a Bank, Business Processing organisation, Hospital, government agency, university, etc., of which the SOC is also a member.

- In these cases, it is also common to find a chief executive officer (CEO) and CIO with cognizance of the entire organization.

Job Role – Analyst Security Operations Centre (SOC)

- An Analyst Security Operations Centre (SOC) in the IT-ITeS Industry is also known as **Engineer SOC**.

- Individuals at this job are responsible for
  - **monitoring and analyzing organizations traffic**
  - **logs for threats**;
  - **notifying potential threats found**;
  - responding to **alarms raised**;
  - following-up for ticket closure with the client and
  - any **enhancements** to existing cyber security measures.

Common Tasks / NOS (National Occupational Standards)

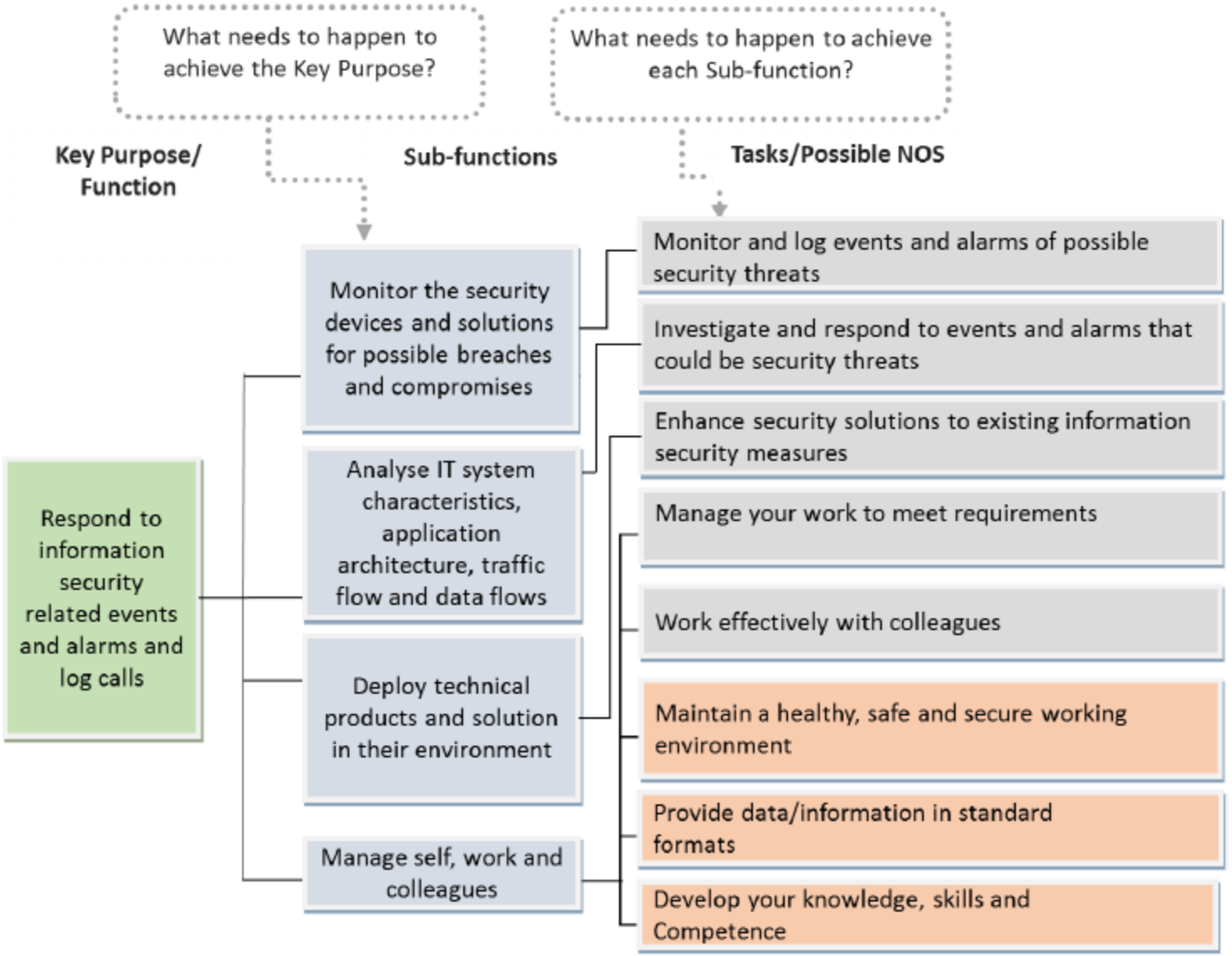


Figure: Functional Analysis of Analyst Security Operations Centre, Source; IT-ITES Sector Skill Council NASSCOM

Analyst SOC

- The job also involves **identifying potential threats** and **performing enhancements to existing cyber security measures** as per specifications or policy guidelines.
- When a security incident is declared they execute incident response process and document the same.
- This job may require the individual to work in a team/shifts.
- The individual should be **result oriented** and have a high attention for detail.
- The individual should also be able to demonstrate good **communication skills and logical thinking**.

Analyst SOC activities

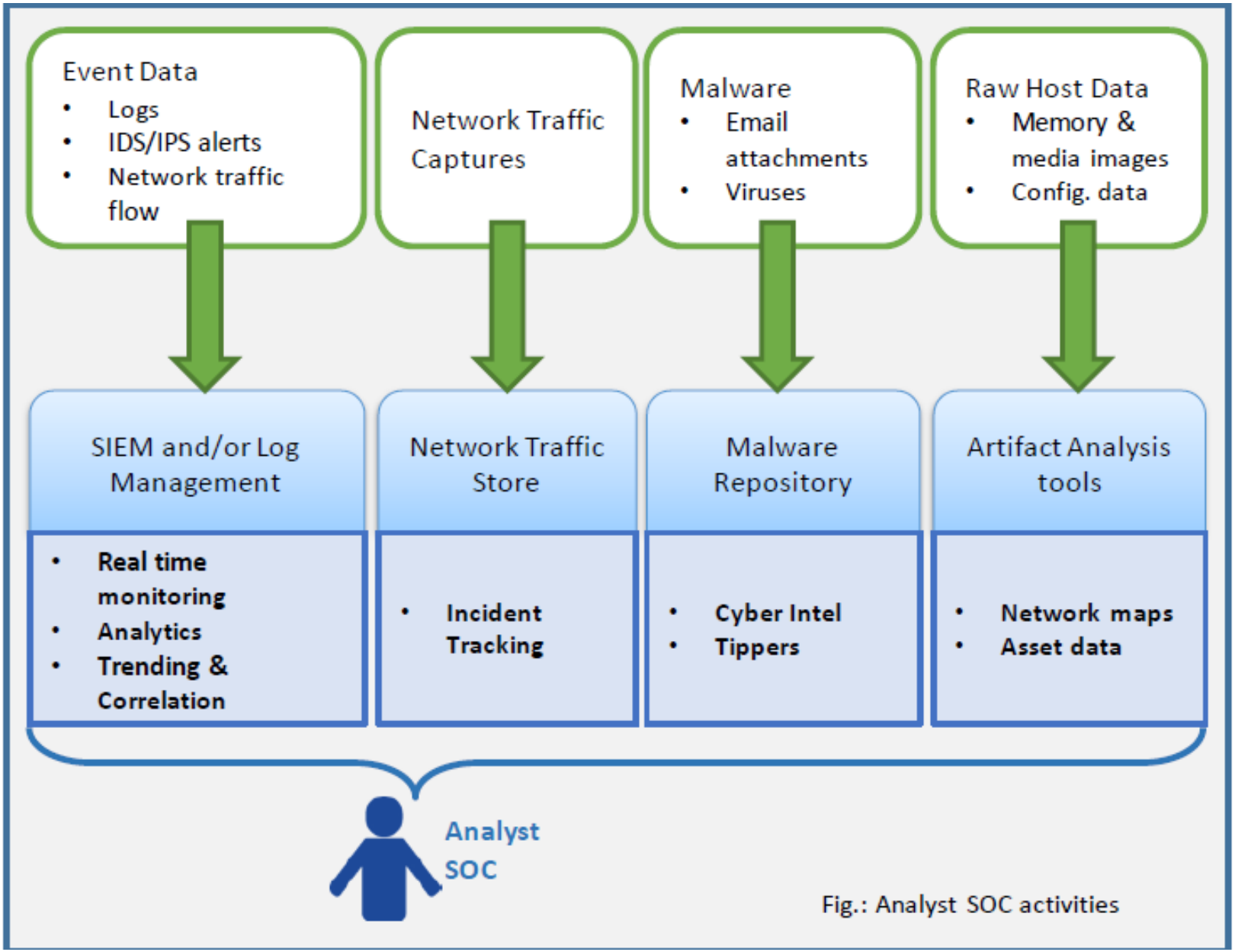


Fig.: Analyst SOC activities

UNIT 1
Monitor and Log Events and Alarms of Possible Security Threats

1.1. Fundamental Concepts
1.1.1 Computer Hardware and Networking Concepts

- **Computer Hardware**
  - Computer is an electro-mechanical device. It takes input from input devices, processes the data according to the input instructions and produces the output via output devices.
  - According to IT ACT 2008, computer is defined as any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.

Computer Hardware and Networking Concepts

- **Computer Program**: a computer program is a set of instructions to perform a specific task.

- **Source Code1**: Every computer program is written in a programming language, such as Java, C/C++, or Perl etc. These programs include anywhere between a few lines to millions of lines of text called source code.

- According to IT ACT 2008, **source code** is defined as "Computer source code means the listing of programs, computer commands, design and layout, and program analysis of computer resource in any form."

How is data stored in a computer?

- The computer manufacturers typically **use two-state (binary i.e. 1 or 0) form, to store data on electronic devices** since it is an engineering convenience of the current technology.

- Two-state systems are **easier to engineer** and two-state logic simplifies several activities.

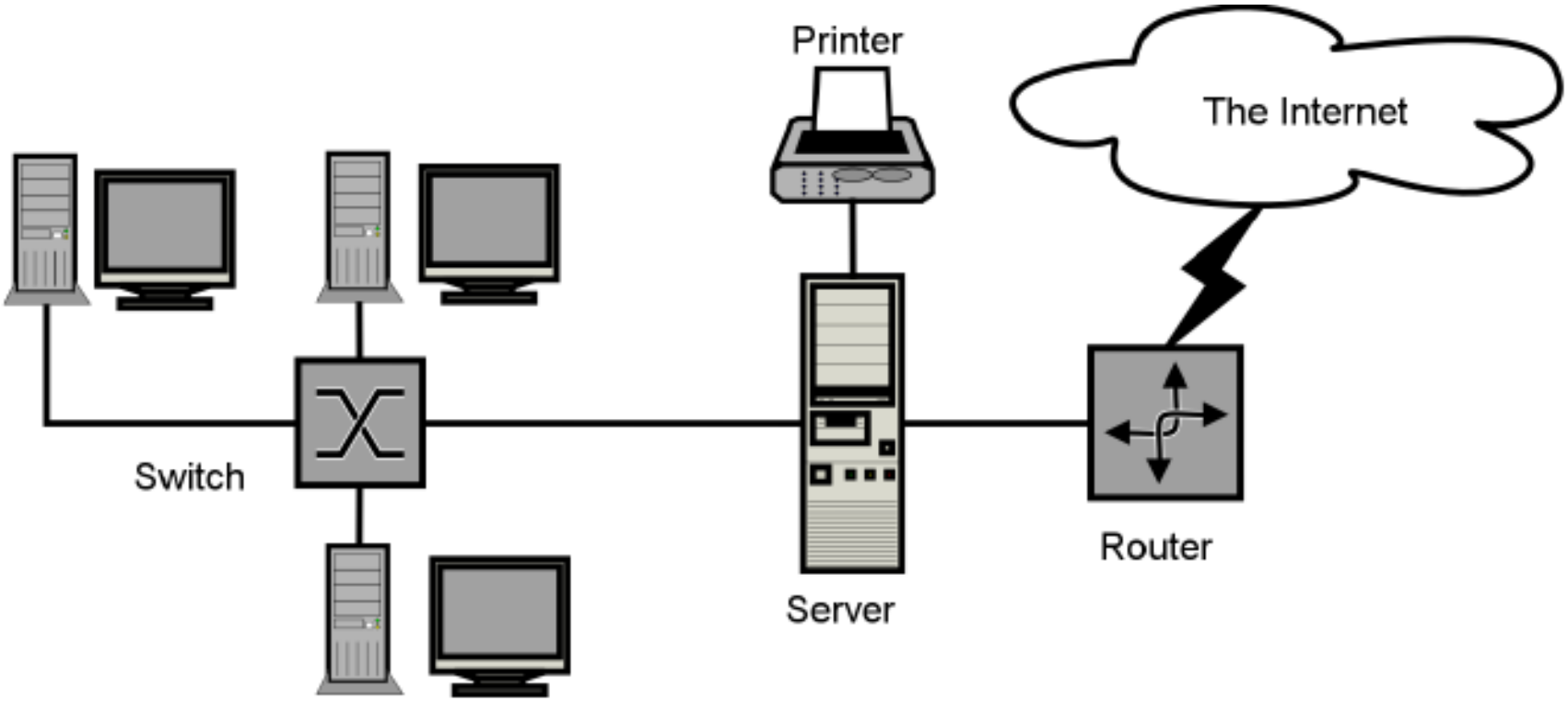
- Each data is stored using some physical device that can be in one of the two stable states:
  - In a **memory chip**, transistor switch may be ON or OFF
  - In a **communications line**, a pulse may be PRESENT or ABSENT [high & low]
  - on a **magnetic disk**, polarity may be POSITIVE or NEGATIVE
  - on a **compact disc**, a pit may be PRESENT or NOT at a particular place

How is data stored in a computer?

- Byte: a byte consists of 8 Bits
- Octet is made up of 8 bits;
- **Nibble** is made up of 4 Bits
- Kilobyte: a kilobyte (KB) consists of 1024 Bytes
- Megabyte: a megabyte (MB) consists of 1024 Kilobytes
- Gigabyte: a gigabyte (gB) consists of 1024 Megabytes
- Terabyte: a Terabyte (TB) consists of 1024 gigabytes

Computer Networking & IP Addresses

- A computer network is a group of computers/devices connected together that share information across a wired/wireless medium.



Computer Networking & IP Addresses

- Each and every computer/device within the network will have two types of addresses-logical and Physical.
  - **Logical addresses** are also known as IP addresses (Internet Protocol addresses).
  - **Physical addresses** are also known as MAC addresses (Media access Control).
- Management and Distribution of IP Addresses
  - IP addresses are managed by the **Internet assigned Numbers authority** (IaNa) which has overall responsibility for the IP address pool and by **the Regional Internet Registries** (RIRs) to which IaNa distributes large blocks of addresses.

Computer Networking & IP Addresses

- The Internet assigned Numbers authority (IaNa) is a department of **The Internet Corporation for assigned Names and Numbers** (ICaNN) responsible for coordinating some key elements that keep the Internet running smoothly.

- The Regional Internet Registries (RIR) manages, distribute, and publicly register IP addresses (and related Internet number resources, such as **autonomous system Numbers** (aNs) and reverse Domain Name system (DNs) within their respective regions.

- They do this according to policies which are developed within their respective regional communities, through open and bottom-up processes.

Regional Internet Registries

There are currently five RIRs:

- AFRINIC, serving the african region
- APNIC, serving the asia Pacific region
- ARIN, serving North america and several Caribbean and North atlantic Islands
- LACNIC, serving latin america and the Caribbean, and
- RIPE NCC, serving Europe, the Middle East, and parts of Central Asia

Internet Registry

- An Internet Registry (IR) is an organization that is responsible for **distributing the IP address space** to its affiliates or customers and for registering those distributions. IRs are classified according to their primary function and territorial scope.

IRs includes:

- APNIC and other Regional Internet Registries (RIRs)
- National Internet Registries (NIRs)
- Local Internet Registries (LIRS), unless the specific context of the reference requires otherwise

National Internet Registry

- A **National Internet Registry** (NIR) primarily allocates address space to its affiliates or constituents, which are generally Local Internet Registries (LIR) organized at a national level.

- NIRs are expected to apply their policies and procedures fairly and equitably to all affiliates of their constituency.

- Note: The National Internet Exchange of India is the neutral meeting point of the ISPS in India.
  - Its main purpose is to facilitate exchange of domestic Internet traffic between the peering ISP members.
  - Its head office is located at Delhi.

Local Internet Registry

- A local Internet Registry (LIR) is generally an Internet service Provider (ISP) and may assign address space to its own network infrastructure and to users of its network services.

- LIR customers may be other “downstream” ISPs which further assign address space to their own customers.

- Figure given below shows the distribution of IP addresses.

Computer Networks

A network is a group of systems that are connected to allow:

a) sharing of resources – such as files or printers or

b) sharing of services such as an Internet connection.

The two aspects of setting up a network are:

a) The Hardware: to connect the systems together and

b) The Software: installed on the computers for communication.

- The network operates by connecting computers and peripherals using two pieces of equipment; switches and routers.

Switches and Routers

- Switches and routers, essential networking basics, enable the devices that are connected to the network to communicate with each other, as well as with other networks.
- **Switches** are used to **connect multiple devices on the same network within a building or campus**.
  - For example, a switch can connect computers, printers and servers, creating a network of shared resources.
  - The switch in one aspect would serve as a controller, allowing the various devices to share information and communicate to each other.
- A Managed switch provides greater flexibility to one's networking basics because the switch can be monitored and adjusted locally or remotely to give him control over network traffic, and who has access to his network.

Switches and Routers

- o An Unmanaged switch works out of the box and does not allow making changes. Home networking equipment typically offers unmanaged switches.

- **Routers** the second valuable component of networking basics are used to tie **multiple networks together**.

- A router is used to **connect networked computers to the Internet** and thereby share an Internet connection among many users.

- Routers, analyze the data being sent over a network, change how it is packaged, and send it to another network, or over a different type of network.

- They connect one's business to the outside world; protect one's information from security threats.

Network Basics

- **Firewall**: Specialized software that examines incoming data and protects business network against attacks

- **Virtual Private Network (VPN)**: A way to allow remote employees to safely access network remotely

- **IP Phone network**: Combine one's company's computer and telephone network, using voice and conferencing technology, to simplify and unify communications.

- **IDS/IPS systems**

An **Intrusion Detection System (IDS)** is designed to monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

An IDS essentially reviews the network traffic and data and identify probes, attacks, exploits and other vulnerabilities.

Intrusion Prevention System (IPS)

- **Intrusion Prevention System (IPS)**, is the next level of security technology with its capability to provide security at all system levels from the operating system kernel to network data packets.

- It provides policies and rules for network traffic along with an IDS for alerting system or network administrators to suspicious traffic, but they leave the action to be taken to the administrator upon being alerted.

- IDS informs of a potential attack, an IPS makes attempts to stop it.

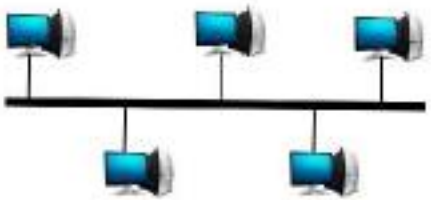
- It has also the capability of being able to prevent known intrusion signatures, but also some unknown attacks due to its database of generic attack behaviors.

Types of Networks

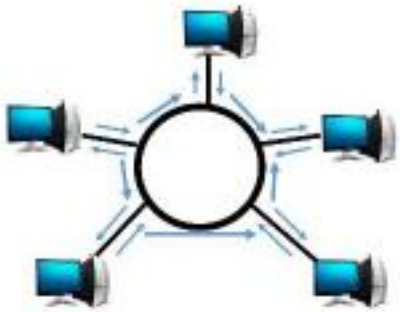
Local Area Network (LAN):

- A LAN is a network that is used for communicating among computer devices, usually within an office building or home.
- They enable the sharing of resources such as files or hardware devices that may be needed by multiple users.
- It is limited in size, typically spanning a few hundred meters, and no more than a mile.
- it is fast, with speeds from 10 Mbps to 10 Gbps.
- It requires little wiring, typically a single cable connecting to each device.
- LAN’s can be either wired or wireless.
- Twisted pair coax or fiber optic cable can be used in wired LAN’s.
- Nodes in a LAN are linked together with a certain topologies

1. **Bus**



2. **Ring**



3. **Star**

LANs are capable of very high transmission rates (100s Mb/s to G b/s).

Wide Area Network (WAN)

- A WAN is a network which covers a large geographic area such as country, continent or even whole of the world.
- A WAN is two or more LANs connected together.
- The LANs can be many miles apart.
- To cover great distances, WANs may transmit data over leased high-speed phone lines or wireless links such as satellites.
- The world's most popular WAN is the Internet.

Personal Area Network (PAN)

- A PAN is a network that is used for communicating among computers and computer devices (including telephones) in close proximity of around a few meters within a room.

- PAN’s can be wired or wireless.

- A personal area network (PAN) is a computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body.

- The devices may or may not belong to the person in question.

- The reach of a PAN is typically a few meters.

Metropolitan Area Network (MAN)

- A MAN often acts as a high speed network to allow sharing of regional resources.
- A MAN typically covers an area of between 5 and 50 km diameter.
- Examples of MAN: Telephone company network that provides a high speed DSL to customers and cable TV network.

- **Another classification of networks** based of no. of workstations on the network is as follows:
- **Peer-to-peer Network:**

A Peer-to-peer network has no dedicated servers, but it has a number of workstations which are connected together for the purpose of sharing information or devices.

All workstations are considered equal, when there are no dedicated servers, any one of them can participate as the client or the server.

Server-Based Networks

- Peer-to-peer networks have a disadvantage that all day-to-day activities can’t be performed at a single place, and data files are stored throughout all the systems.

- Server based networking overcomes the problems in peer-to-peer networking by storing all the data files on the network.

- The network also stores a list of users who may use the network resources and usually holds the resources as well.

Server-Based Networks

- The server in a server-based network may provide a number of different services:
  - File and print servers
  - Application servers
  - Web servers
  - Directory servers

File and print servers

- *File and print servers* control and share printers and files among clients on the network.
- The files are placed on a server to be accessible to a large network of users.
- Files servers often have the following characteristics:
  - Large amount of memory
  - Fast hard disks
  - Multiple CPUs
  - Fast I/O buses
  - High-capacity tape drives
  - Fast network adapters
  - Redundant power supplies
  - Hot-swappable hard disks and power supplies

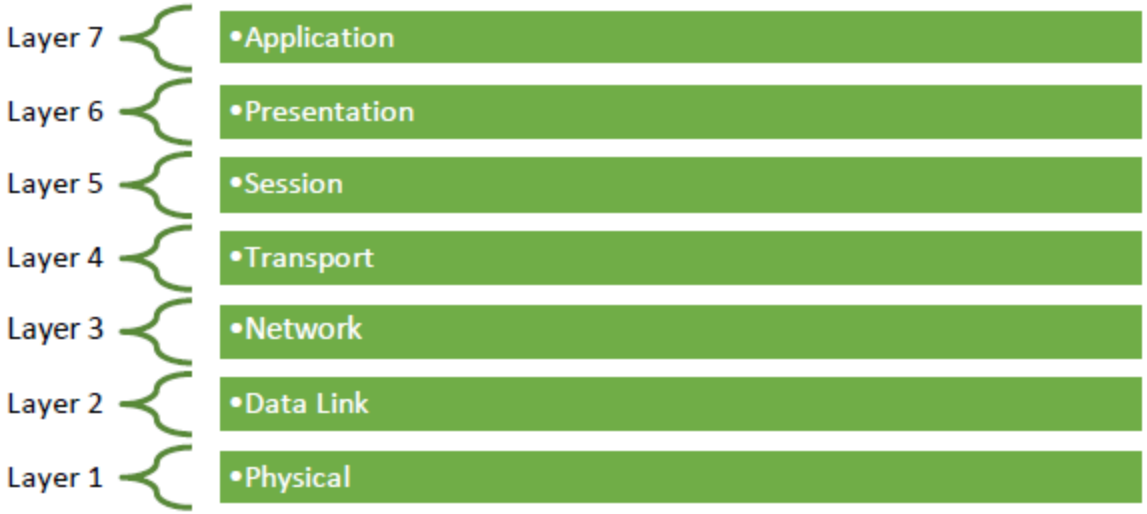
- *Application servers* are servers that run some form of special program on the server.
- An example of an application server is a server that runs the company's email server.
- The email server software is special software that can be run on a server operating system.
- Another example of software that would run on an application server is a database server product such as Microsoft SQL Server.

- *Web Servers* are servers that run the Hypertext Transfer Protocol (HTTP) and are designed to publish information on the Internet or the corporate intranet.
- They are popular in today's business as they **host web applications** (websites) for the organization.
- They could be designed for internal use, or used to publish information to the rest of the world on the internet.
- Examples of web server software are Microsoft's Internet Information Services that runs on **Windows or Apache web server software** that runs on **UNIX/Linux, Novell NetWare, and Windows**.

OSI Model

- The Open System Interconnection (OSI) model defines a networking framework to implement protocols in seven layers.

- In the OSI model, control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.



Layer 1: Physical Layer

The physical layer has the following major functions:

- It defines the electrical and physical specifications of the data connection and also the relationship between a device and a physical transmission medium (e.g., a copper or fiber optical cable, radio frequency). This includes the layout of pins, voltages, line impedance, cable specifications, signal timing and similar characteristics for connected devices and frequency (5 GHz or 2.4 GHz etc.) for wireless devices.
- It defines transmission mode i.e. simplex, half-duplex, full duplex.
- It defines the network topology as bus, mesh, or ring being some of the most common.
- Encoding of bits is done in this layer.
- It determines whether baseband (digital) or broadband (analog) signaling will transmit the encoded bits.
- It mostly deals with raw data.

The physical layer of Parallel SCSI operates in this layer, as do the physical layers of Ethernet and other local-area networks, such as Token Ring, FDDI, ITU-T G.hn, and IEEE 802.11 (Wi-Fi), as well as personal area networks such as Bluetooth and IEEE 802.15.4.

Layer 2: Data Link Layer

The data link layer provides node-to-node data transfer—a link between two directly connected nodes. It detects and possibly corrects errors that may occur in the physical layer. It defines the protocol to establish and terminate a connection between two physically connected devices. It also defines the protocol for flow control between them.

IEEE 802 divides the data link layer into two sub layers:

- Media Access Control (MAC) layer - responsible for controlling how devices in a network gain access to medium and permission to transmit it.
- Logical Link Control (LLC) layer - responsible for identifying Network layer protocols and then encapsulating them and controls error checking and frame synchronization.

The MAC and LLC layers of IEEE 802 networks such as 802.3 Ethernet, 802.11 Wi-Fi, and 802.15.4 ZigBee, operate at the data link layer.

The Point-to-Point Protocol (PPP) is a data link layer that can operate over several different physical layers, such as synchronous and asynchronous serial lines.

The ITU-T G.hn standard, which provides high-speed local area networking over existing wires (power lines, phone lines and coaxial cables), includes a complete data link layer that provides both error correction and flow control by means of a selective-repeat sliding-window protocol.

Layer 3: Network Layer

The network layer provides the functional and procedural means of transferring variable length data sequences (called datagrams) from one node to another connected to the same network. It translates logical network address into physical machine address. It is a medium to which many nodes can be connected; on which every node has an address.

Message delivery at the network layer is not necessarily guaranteed to be reliable; a network layer protocol may provide reliable message delivery, but it need not do so. A number of layer-management protocols, a function defined in the management annex, ISO 7498/4, belong to the network layer. These include routing protocols, multicast group management, network-layer information and error, and network-layer address assignment. It is the function of the payload that makes these belong to the network layer, not the protocol that carries them.

Layer 4: Transport Layer

The transport layer provides the functional and procedural means of transferring variable-length data sequences from a source to a destination host via one or more networks, while maintaining the quality of service functions.

An example of a transport-layer protocol in the standard Internet stack is Transmission Control Protocol (TCP), usually built on top of the Internet Protocol (IP). The transport layer controls the reliability of a given link through flow control, segmentation/de-segmentation, and error control. They can keep track of the segments and retransmit those that fail. It also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred.

The transport layer creates packets out of the message received from the application layer. Packetizing is a process of dividing the long message into smaller messages. OSI defines five classes of connection-mode transport protocols ranging from class 0 (which is also known as TP0 and provides the fewest features) to class 4 (TP4, designed for less reliable networks, similar to the Internet). Class 0 contains no error recovery, and was designed for use on network layers that provide error-free connections. Class 4 is closest to TCP, although TCP contains functions, such as the graceful close, which OSI assigns to the session layer. Also, all OSI TP connection-mode protocol classes provide expedited data and preservation of record boundaries.

Roughly speaking, tunnelling protocols operate at the transport layer, such as carrying non-IP protocols such as IBM's SNA or Novell's IPX over an IP network, or end-to-end encryption with IPsec. While Generic Routing Encapsulation (GRE) might seem to be a network-layer protocol, if the encapsulation of the payload takes place only at endpoint, GRE becomes closer to a transport protocol that uses IP headers but contains complete frames or packets to deliver to an endpoint. L2TP carries PPP frames inside transport packet.

Although not developed under the OSI Reference Model and not strictly conforming to the OSI definition of the transport layer, the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) of the Internet Protocol Suite are commonly categorized as layer-4 protocols within

Layer 5: Session Layer

The session layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes check-pointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session check-pointing and recovery, which is not usually used in the Internet Protocol Suite. The session layer is commonly implemented explicitly in application environments that use remote procedure calls.

Layer 6: Presentation Layer

The presentation layer establishes context between application-layer entities, in which the application-layer entities may use different syntax and semantics if the presentation service provides a big mapping between them. If a mapping is available, presentation service data units are encapsulated into session protocol data units, and passed down the protocol stack.

This layer provides independence from data representation (e.g., encryption) by translating between application and network formats. The presentation layer transforms data into the form that the application accepts. This layer formats and encrypts data to be sent across a network. It is sometimes called the syntax layer.

Layer 7: Application Layer

The application layer is the OSI layer closest to the end user, which means both the OSI application layer and the user interact directly with the software application. It also interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model.

Application-layer functions typically include:

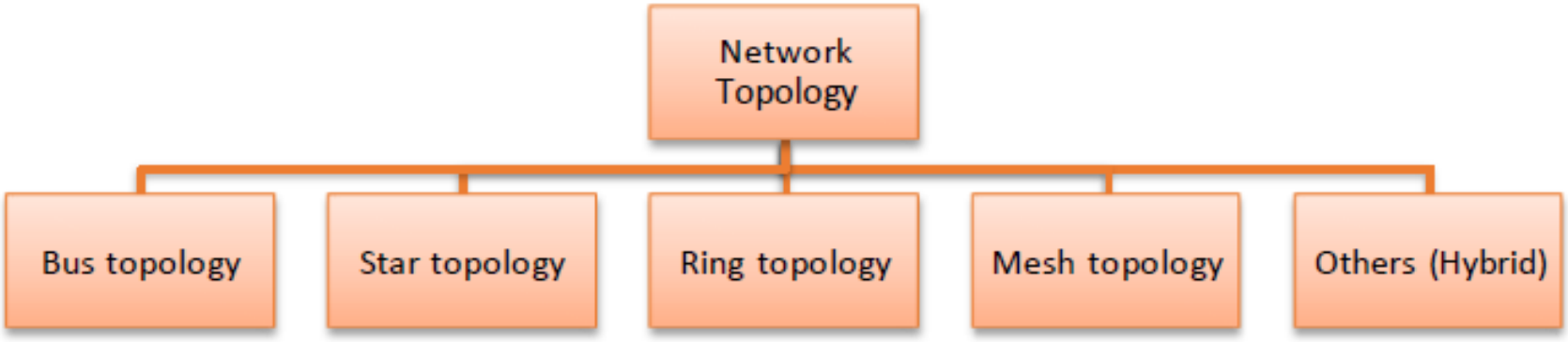
- identifying communication partners
- determining resource availability
- synchronizing communication

Identifying communication partners: the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network or the requested communication exists. In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer.

This layer supports application and end-user processes. Everything at this layer is application-specific. The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

In CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. If two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

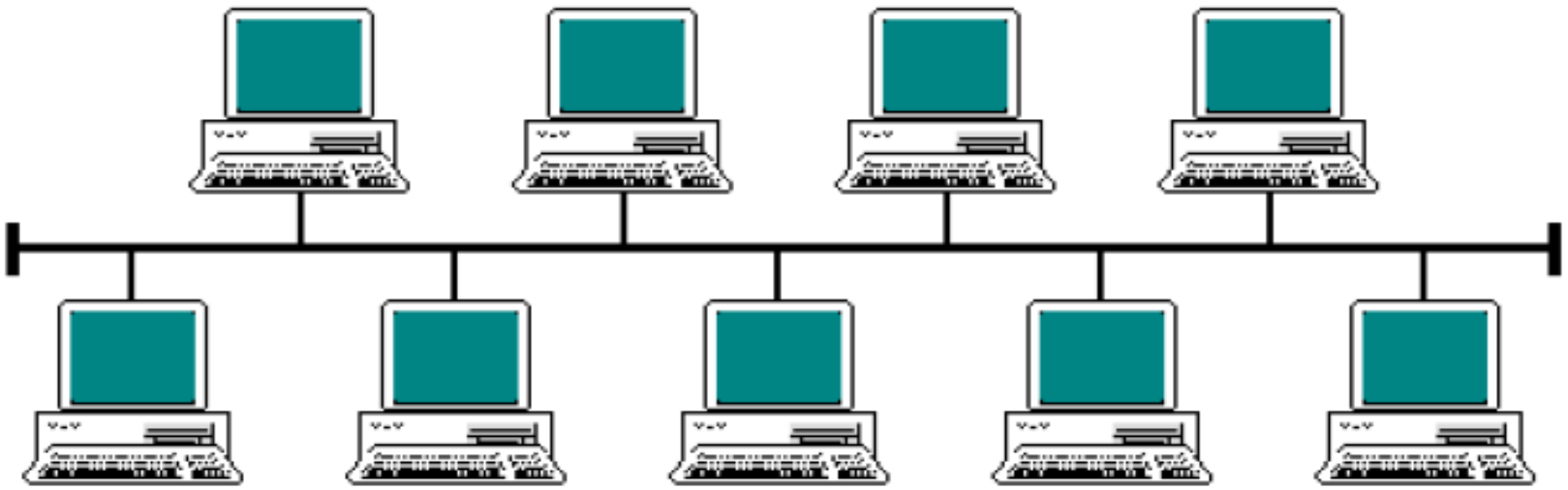
Network Topology



Bus Topology

This network topology is also referred to as a linear bus. The core element of a bus topology is a single cable to which all nodes are connected via short connecting cables. This topology makes it extremely easy to add other subscribers to the network.

Information is transmitted by the individual bus subscribers in the form of so-called messages and distributed over the entire bus. Nodes transmit and receive messages. If a node fails, the data that is expected from this node is no longer available to the other nodes on the network. However, the remaining nodes can continue to exchange information. However, a network with a bus topology fails completely if the main line is defective (due to a cable break, for example).

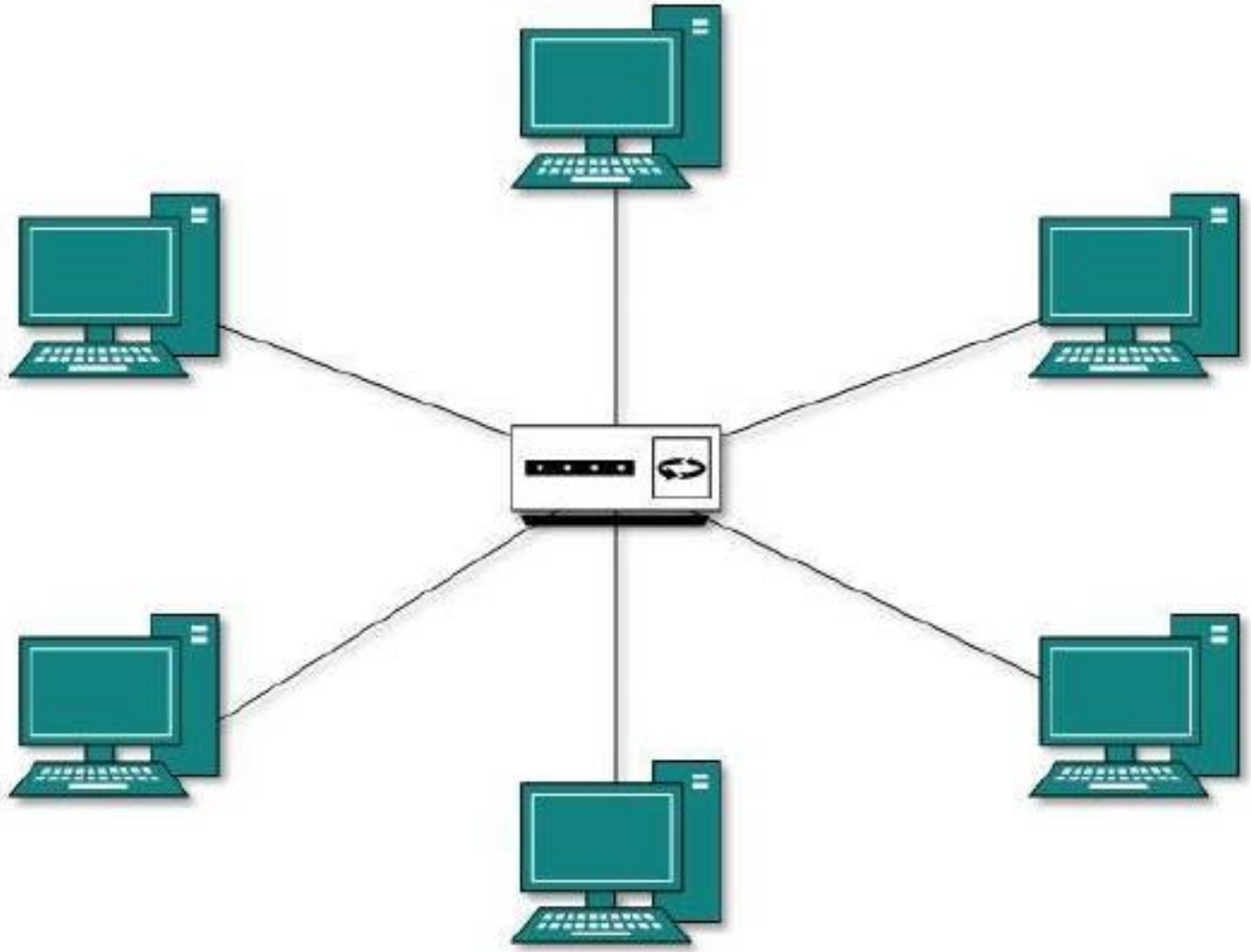


Star Topology

The star topology consists of a main node (repeater, hub) to which all other nodes are coupled via a single connection. A network with this topology is therefore easy to extend if free capacity is available (connections, cables).

In star topologies, data is exchanged between the individual node connections and the main node, whereby a distinction is made between active and passive star topologies. In active star topologies, the main node contains a computer that processes and relays information. The performance capability of a network is essentially determined by the performance capability of this computer. However, the main node does not have to have special control intelligence. In passive star systems, it merely connects the bus lines of the network subscribers together. The following applies to active and passive stars: if a network subscriber fails or a connecting line to the main node is defective, the rest of the network continues to operate.

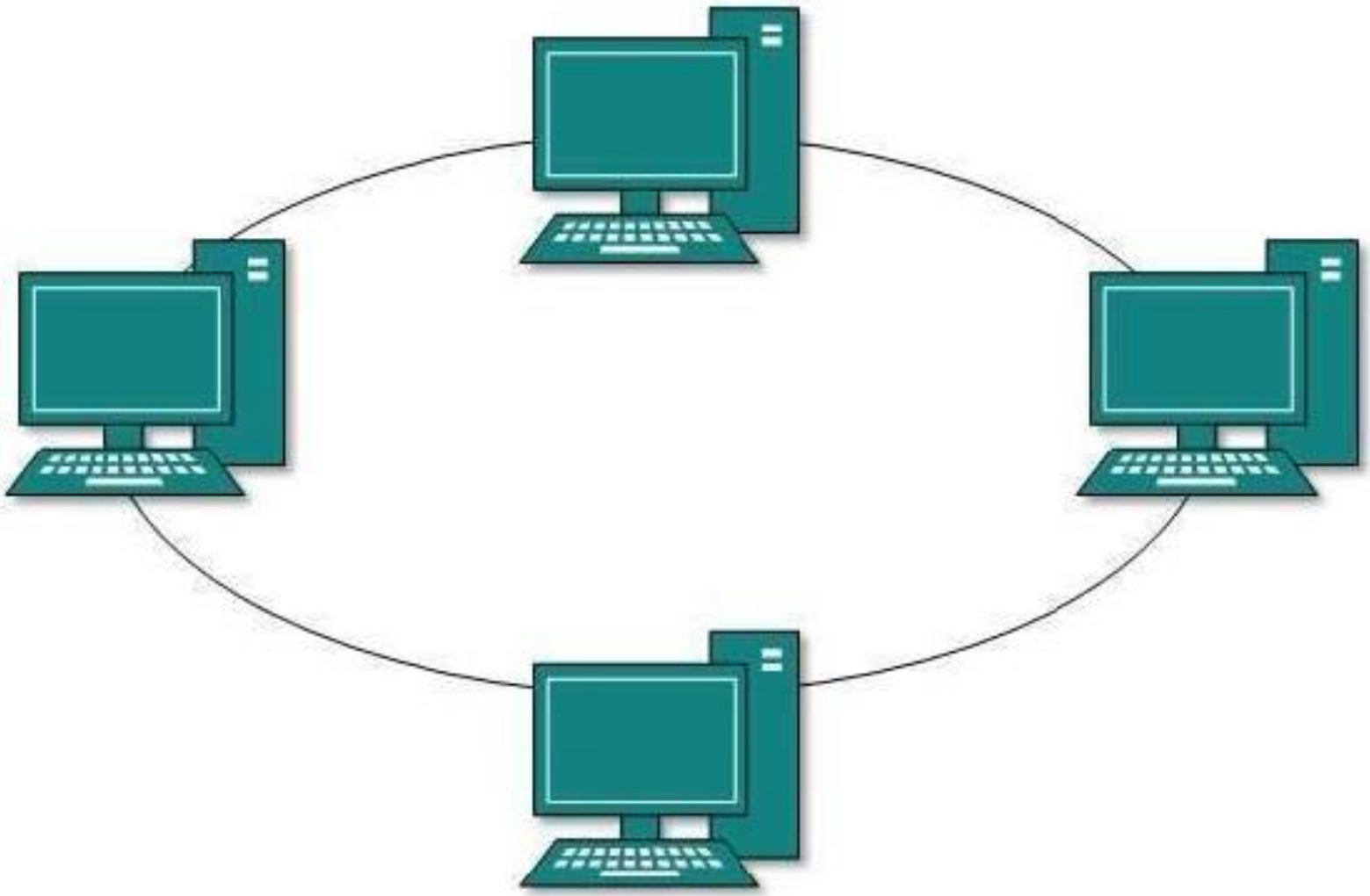
However, if the main node fails the entire network is disabled. In the automotive area, star structures are under discussion for safety and security systems such as brakes and steering. In this case, the risk of a complete network failure is prevented by designing the main node to be physically redundant. This means that several main nodes are used to which the nodes whose information is needed for safe operation of the vehicle can be connected in parallel.



Ring Topology

In the ring topology, each node is connected to its two neighbors. This creates a closed ring. A distinction can be made between single rings and double rings. In a single ring, data transfers are unidirectional from one station to the next. The data is checked when it is received. If the data is not intended for this station it is repeated (repeater function), boosted and relayed to the next station. The data that is being transferred is therefore relayed from one station to the next in the ring until it has reached its destination or arrives back at its point of origin, where it will then be discarded. As soon as a station in a single ring fails, the data transfer is interrupted and the network breaks down completely.

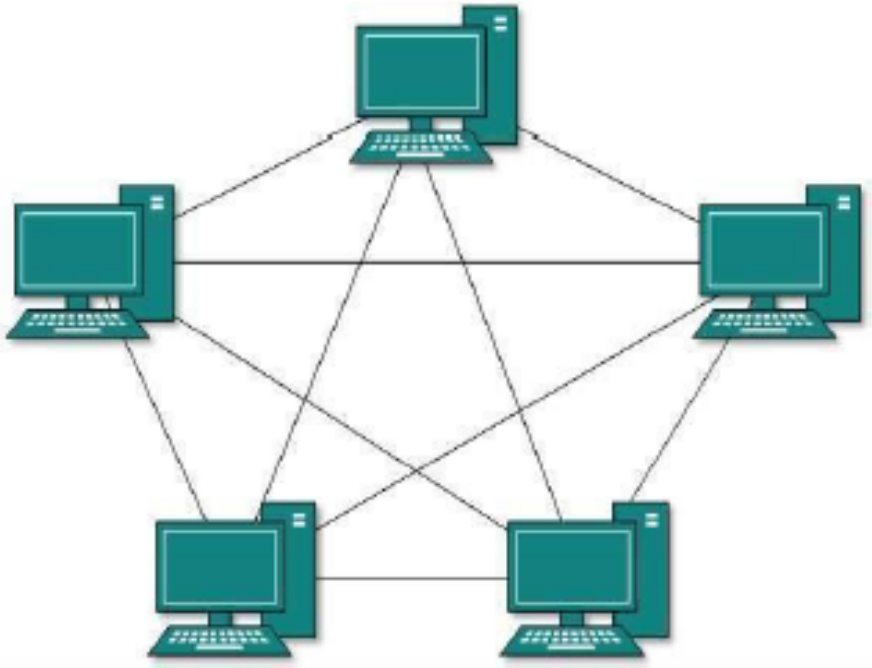
Rings can also be set up in the form of a double ring (e.g. FTTI), in which the transfer of data is bidirectional. In this topology, the failure of a station or a connection between two stations can be overcome, since all data is still transferred to all operational stations in the ring. However, if several stations or connections fail, the possibility of a malfunction cannot be ruled out.



Mesh Topology

In a mesh topology, each node is connected to one or more other nodes. In a fully meshed network, each node is connected to every other node. If a mode or connection fails, it is possible for the data to be rerouted.

This type of network therefore has a high degree of system stability. However, the cost of networking and transporting the message is high. Radio networks form a type of mesh topology, since the transmissions from each station are received by every other station that is within range. A mesh topology is bus-like as far as exchanging messages is concerned, and star-like regarding data transfers, since every station receives all transmissions from every other station, but connection failures can be overcome.



Hybrid Topologies

Hybrid topologies are a combination of different network topologies. Examples of such combination are:

- **Star bus topology:** the hubs of several star networks are interconnected as a linear bus.
- **Star ring topology:** the hubs of several star networks are connected to the main hub. The hubs of the star network are connected in the form of a ring in this main hub.

Wireless Topologies

A wireless topology is one in which few cables are used to connect systems. The network is made up of transmitters that broadcast the packets using radio frequencies. The network contains special transmitters called cells, or wireless access points, which extend a radio sphere in the shape of a bubble around the transmitter. This bubble can extend to multiple rooms and possibly floors in a building. The PCs and network devices have a special transmitter-receiver, which allows them to receive broadcasts and transmit requested data back to the access point. The access point is connected to the physical network by a cable, which allows it, and any wireless clients, to communicate with systems on the wired network.

In Wireless topology the wireless cells, or access points, are connected to the network by connecting into the hub or switch that has a connection to the rest of the wired network. These are wireless clients, and they will get access to the network through the wireless cell (or access point).

Another option for wireless networks is the use of a radio antenna on or near the building, which allows one cell to cover the building and the surrounding area. Wireless networks also can consist of infrared communications, similar to a remote-control TV, but this type of communication is slow and requires a direct line of sight—as well as close proximity—for the communication to work. Infrared mainly is used only between two systems. It is useful between laptops or a laptop and a printer.

Advantages of a Wireless Topology:

- The wireless network requires only base backbone segments to connect the wireless cells to the wired network if there is one. Once these are set up, the PC and network devices also need the special transmitter-receiver network interface cards to allow the PCs and devices to communicate with the cell and then through the cell to the servers.
- Troubleshooting failed devices and cells is very easy and makes failed components easy to find and replace.

Disadvantages of a Wireless Topology:

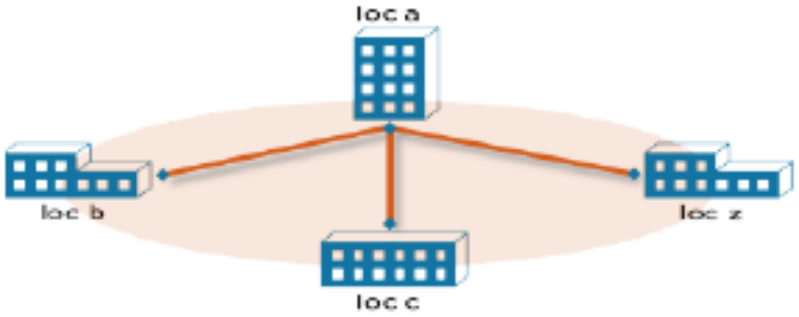
- Chance of signal interference, blockage, and interception: Other devices and machinery that emit radio frequencies or "noise" can cause interference and static, which can disrupt the bubble of communication around the cell.
- Another source of noise is lightning during storms. This noise is the same static; one hears when lightning strikes while he is speaking on a phone. Blockage can occur in structures that are made of thick stone or metal, which do not allow radio frequencies to pass through easily.
- Another major disadvantage with wireless is signal interception. Signal interception means unwanted third parties could intercept wireless communications without physically being on the premises; they would simply have to be within the signal range.

There are two popular layouts for topologies:

1. **Point-to-point (Host to Host):** one system connected directly to another system. In the past these systems would connect directly through the serial ports with a null modem cable, but these days, one could connect them using a crossover cable or a wireless connection.

Point-to-Point

2. **Point-to-multipoint**: A point-to-multipoint topology uses a central device that connects all the devices together. This topology is popular with wireless. With point-to-multipoint, when the central device sends data, it is received by all devices connected to the central device. But if one of the devices that are connected sends data, then it is received by only the destination system.



Point-to-MultiPoint

Segments and Backbones

- A **network segment** is a cable length (or multiple cable lengths) that is uninterrupted by network connectivity devices, such as bridges and routers.

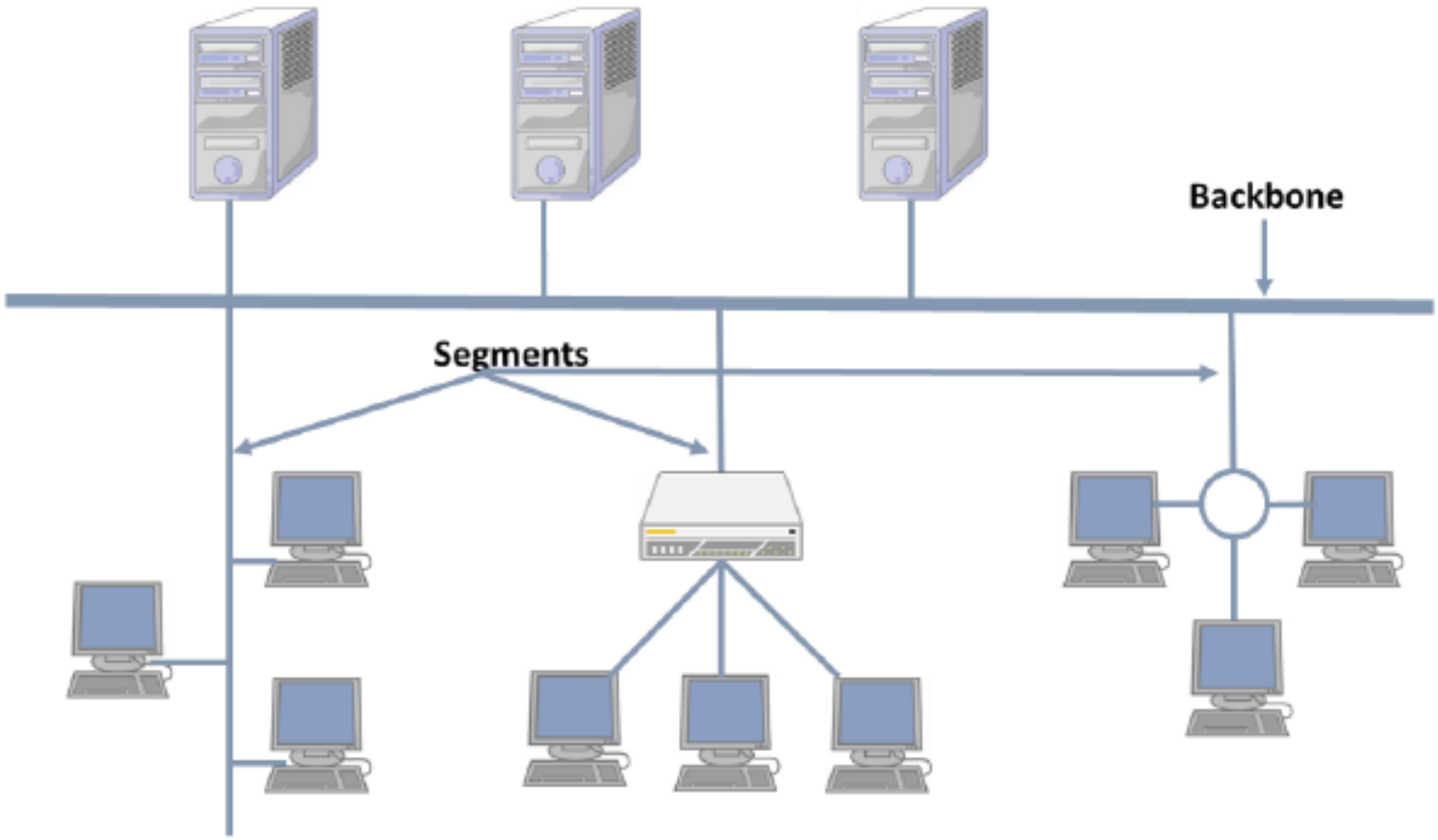
- It is typical that a single network may be broken into multiple network segments through the use of a bridge or router to cut down on network traffic.

- In figure, there are three network segments. Also notice that each network segment could have a number of clients and servers all connected through a number of hubs that are then connected to a backbone.
- This is just one possible solution involving network segments.

Backbone

- A **backbone** is the main cable segment or trunk in the network.
- In a bus network, one might see a main cable trunk that has smaller cables connecting the workstations.
- These smaller cables, known as **drop cables**, connect the workstations to the backbone.
- Another example of a backbone is a satellite linking geographically dispersed local area networks (LANs), making a wide area network (WAN).
- Such a backbone is an example of a wireless communications network, whereas the previous examples all used cable as the medium.

Network Backbone



Network Organization

Addressing

- In order to make it possible to transmit messages via a network and evaluate the contents thereof, the useful data (payload) that is transmitted is also accompanied by data transfer information.

- This can be explicitly contained within the transmission or implicitly defined using pre-set values.

- Addressing represents important information for data transfer information.

- It is needed in order for a message to be sent to the correct recipient. There are different ways of doing this.

Subscriber-oriented method

- The data is exchanged on the basis of node addresses. The message sent by the transmitter contains the data to be transmitted and also the destination node address.

- All receivers compare the transmitter receiver address to their own address, and only the receiver with the correct address evaluates the message.

- The majority of conventional communication systems (such as Ethernet) operate using the **subscriber addressing principle**.

Message-oriented method

- In this method it is not the receiver node that is addressed, but the message itself.

- Depending on the content of the message, it is identified by a message identifier that has been predefined for this message type.

Transmission-oriented method

- Transmission characteristics can also be used to identify a message.

- If a message is always transmitted within a defined time window, it can be identified on the basis of this position.

- By way of a safeguard, this addressing is often combined with message or subscriber-oriented addressing.

Bus access method

- A node must access the bus in order to transmit a message. In the bus access method, a distinction is made between
- **Predictable methods** in which the bus access is determined by certain time dependent network characteristics, whereby only one node can transmit at a time.
- In this method the bus access right is determined before bus access.
- It can thereby be ensured that only one subscriber is using the bus at a time.
- Access collisions because of simultaneous bus usage will be prevented if all subscribers use this method.

Random Methods

- **Random methods** whereby any node can attempt to transmit data if the bus appears to be free.

- In the random method, the nodes can simultaneously attempt to use the bus as soon as it appears to be free. The timing of the bus access is therefore random.

- There is a risk of transmission collisions using this method, which will require attention.

- This can be dealt with by repeating transmissions after a collision has been detected (e.g. Ethernet),by giving the transmissions different coding (CDMA), controlling communication via a master or prioritizing message types or transmitters.

Time Division Multiple Access (TDMA)

- TDMA is a deterministic (predictive) access method.
- In this case each node is assigned a time window in which it is allowed to transmit (a priori).
- A fixed schedule is therefore required for the network.
- There is not usually a main communication subscriber controlling the communication procedure.
- The internal clocks of the different stations must run extremely synchronously with TDMA, since the transmit windows have to be adhered to with extreme precision.

Time Division Multiple Access (TDMA)

- **Master-slave**: In the master-slave system, one node on the network operates as the master.
- This node determines the communication frequency by interrogating its subordinate nodes (slaves).
- A slave only replies if it is spoken to by the master.
- However, some master-slave protocols allow a slave to contact a master in order to transmit a message (e.g. transmit information about the position of the power-window unit to the door module).

Time Division Multiple Access (TDMA)

- **Multi-master**: In a Multi-master network, several nodes can access the transport medium independently without the assistance of another node.

- Bus access is uncontrolled. Every node can access the bus and transmit a message if the bus appears to be free.

- This means that each node is its own master, and that any node can start a message transfer with equal status.

- However, this also means that collision detection and handling methods have to be in place.

Network Protocols

- The Internet protocol suite is the computer networking model and set of communications protocols used on the Internet and similar computer networks. It is commonly known as TCP/IP,

- because its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP) were the first networking protocols defined in this standard.

- It is occasionally known as the DoD model (Department of Defence), because the development of the networking model was funded by DARPA, an agency of the United States Department of Defence.

TCP/IP

- TCP/IP provides end-to-end connectivity specifying how data should be packetized, addressed, transmitted, routed and received at the destination.

- This functionality is organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.

- From lowest to highest, the layers are the link layer, containing communication methods for data that remains within a single network segment (link); the internet layer, connecting independent networks, thus establishing inter-networking; the transport layer handling host-to-host communication; and the application layer, which provides process-to-process data exchange for applications.

TCP/IP

- The TCP/IP model and many of its protocols are maintained by the Internet Engineering Task Force (IETF).

TCP/IP	OSI MODEL	PROTOCOLS
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP, POP3, RTP, TRSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

Thank You !!!!!!!

UNIT I
Information Security and Threats

Submitted by

Dr. P. Vijayakumar

Associate Professor / School of Electronics Engineering

Vellore Institute of Technology

Chennai

Content

- Introduction to Information Security
- Information Assets & Threats
- Common Vulnerabilities and Exposures (CVE).
- Elements of Information Security
- Principles and Concepts – Data Security
- Types of Controls

Introduction to Information Security

- With the pervasive growth and use of digital information, much of which is confidential, there has also been growth in **incidents of information theft**, including **cyber attacks by hackers**.

- This has happened both in **governments and in private companies**.

- This has necessitated the need for the position of **information security analyst**.

Introduction to Information Security

- Those who work as information security analysts are responsible **for keeping information safe from data breaches** using a **variety of tools and techniques**. Information security analysts protect information stored on **computer networks, in applications** etc.

- They do this with **special software** that allows them **to keep track** of those who **can access** and who have **accessed data**.

- Also, they may **perform investigations** to determine whether or not **data has been compromised**, the extent of it and related vulnerabilities.

Introduction to Information Security

- Someone at an **entry level positi**on may operate the software to monitor and analyze information.

- At **senior level positions**, one may carry out investigative work to **determine whether a security breach** has occurred.

- At **higher levels people** design systems and architecture to **address these vulnerabilities**.

Introduction to Information Security

- The field of information security has seen **significant growth** in recent times, and the number of **job opportunities** in this area are likely to increase in the near future.

- Recent **incidents of information theft from large companies** like Target, Sony and Citibank has shown the risks and challenges of this field and this necessitates the growing need for information security and professionals in this field.

- We are now witnessing the rising background level of **data leakage from** governments, businesses and other organisations, families and individuals.

- A larger part of an information security analyst's work involves **monitoring data use and access on a computer network**.

Security analysts focus on three main areas:

1. **risk assessment** (identifying risks or issues an organization may face)

2. **vulnerability assessment** (determining an organization's weaknesses to threats)

3. **defense planning** (designing the protection architecture and installing security systems such as firewalls and data encryption programs)

Introduction to Information Security

- Information security analysts can find themselves working with **IT companies, financial and utility companies and consulting firms.**

- They may also find positions with government organizations.

- Any company or organization with **data to protect may hire information security analysts** so they could find themselves working at a wide variety of different institutions.

- A number of companies operate '**Security Operation Centres** (SOCs)' for carrying out data security services for captive or client services.

Major Skills of Security Analyst

- Understanding security policy
- Data & Traffic Analysis
- Identifying Security Events –> How & when to alarm
- Incident Response

Foundation and Background

- Network infrastructure knowledge
- Diverse device configuration ability
- Security configuration knowledge
- Data management & teamwork

Challenges for Security Analyst

- Not tied to a product or solution
- Complex knowledge – Not one specific process is correct or product solution
- Diverse set of skills are needed

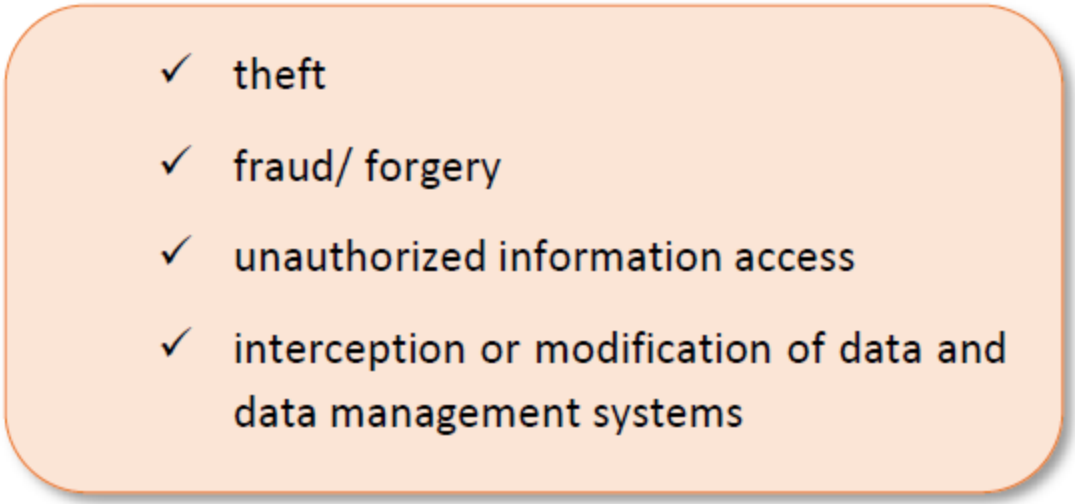
Information Assets & Threats

- Security concerning IT and information is normally categorised in three categories to facilitate the management of information.

Confidentiality	Integrity	Availability
• Prevention of unauthorized disclosure or use of information assets	• Prevention of unauthorized modification of information assets	• Ensuring authorized access of information assets when required for the duration required

Threats to information assets

- **Risk** is the potential threat, and process of **understanding and responding** to factors that may lead to a **failure** in the **confidentiality, integrity or availability** of an information system constitute **risk management**.
- The key concerns in information assets security are:



Threats to information assets

- **Vulnerabilities** is a **weakness** in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
- '**Threat agent or actor**' refers to the **intent and method targeted** at the intentional exploitation of the vulnerability or a **situation and method** that may accidentally trigger the vulnerability.
- A '**threat vector**' is a **path or a tool** that a threat actor uses to attack the target.
- '**Threat targets**' are **anything of value to the threat actor** such as PC, laptop, PDA, tablet, mobile phone, online bank account or identity

Threat classification

Microsoft has proposed a threat classification called STRIDE from the initials of threat categories:

- Spoofing of user identity
- Tampering
- Repudiation
- Information disclosure (privacy breach or data leak)
- Denial of Service (D.o.S.)
- Elevation of privilege

Threat agents (individuals and groups) can be classified as follows:

- Non-Target specific: Non-Target specific threat agents are computer viruses, worms, Trojans and logic bombs.
- Employees: staff, contractors, operational/ maintenance personnel or security guards who are annoyed with the company.
- Organized crime and criminals: criminals target information that is of value to them, such as bank accounts, credit cards or intellectual property that can be converted into money.
- Criminals will often make use of insiders to help them.
- Corporations: corporations are engaged in offensive information warfare or competitive intelligence. Partners and competitors come under this category.
- Unintentional human error: accidents, carelessness etc.
- Intentional human error: insider, outsider etc.
- Natural: Flood, fire, lightning, meteor, earthquakes etc.

Types of attacks

- **Virus :** Virus is a malicious program able to inject its code into other programs/ applications or data files and the targeted areas become "infected".

- Installation of a virus is done without user's consent, and spreads in form of executable code transferred from one host to another.

- Types of viruses include Resident virus , non-resident virus; boot sector virus; macro virus; file-infecting virus (file infector); Polymorphic virus; Metamorphic virus; Stealth virus; Companion virus and Cavity virus.

Worm

- Worm is a malicious program category, exploiting operating system vulnerabilities to spread itself.
- In its design, worm is quite similar to a virus - considered even its sub-class.
- Unlike the viruses though worms can reproduce/ duplicate and spread by itself.
- During this process worm does not require to attach itself to any existing program or executable.
- Different types of worms based on their method of spread are email worms; internet worms; network worms and multi-vector worms.

Trojan

- Computer Trojan or Trojan Horses are named after the mythological Trojan horse owing to their similarity in operation strategy.

- Trojans are a type of malware software that masquerades itself as a not-malicious even useful application but it will actually do damage to the host computer after its installation.

- Unlike virus, Trojans do not self-replicate unless end user intervene to install.

Types of Virus

- **Resident virus** - virus that embeds itself in the memory on a target host. In such way it becomes activated every time the OS starts or executes a specific action.

- **Non-resident virus** - when executed, this type of virus actively seeks targets for infections either on local, removable or network location. Upon further infection it exits. This way is not residing in the memory any more.

- **Macro virus** - virus written in macro language, embedded in Word, Excel, Outlook etc. documents. This type of virus is executed as soon as the document that contains it, is opened. This corresponds to the macro execution within those documents which under normal circumstances is automatic.

Types of Virus

- **File-infecting virus (file-infector)** – this is a classic form of virus.

- When the infected file is being executed, the virus seeks out other files on the host and infects them with malicious code.

- The malicious code is inserted either at the beginning of the host file code (prepending virus), in the middle (mid-infector) or in the end (appending virus).

Types of Virus

- A specific type of viruses called "**cavity virus**" can even inject the code in the gaps in the file structure itself.
- The start point of the file execution is changed to the start of the virus code to ensure that it is run when the file is executed.
- Afterwards the control may or may not be passed on to the original program in turn.
- Depending on the infections routing the host file may become otherwise corrupted and completely non-functional.
- More sophisticated viral forms allow through the host program execution while trying to hide their presence completely (see polymorphic and metamorphic viruses).

Types of Virus

- **Metamorphic virus -** this virus is capable of changing its own code with each infection.

- The rewriting process may cause the infection to appear different each time but the functionality of the code remains the same.

- The metamorphic nature of this virus type makes it possible to infect executable from two or more different operating systems or even different computer architectures as well.

- The metamorphic viruses are ones of the most complex in build and very difficult to detect.

Types of Virus

- **Stealth virus** - memory resident virus that utilises various mechanisms to avoid detection.

- This avoidance can be achieved for example, by removing itself from the infected files and placing a copy of itself in a different location.

- The virus can also maintain a clean copy of the infected files in order to provide it to the antivirus engine for scan while the infected version still remains undetected.

- Furthermore, the stealth viruses are actively working to conceal any traces of their activities and changes made to files.

- **Multipartite virus** – this attempts to attack both the file executable as well as the master boot record of the drive at the same time.
- This type may be tricky to remove as even when the file executable part is clean it can re-infect the system all over again from the boot sector if it wasn't cleaned as well.

- **Camouflage virus** – this virus type is able to report as a harmless program to the antivirus software.
- In such cases where the virus has similar code to the legitimate non-infected files code the antivirus application is being tricked that it has to do with the legitimate program as well.

- This would work only but in case of basic signature based antivirus software.

- Nowadays, antivirus solutions have become more elaborate whereas the camouflage viruses are quite rare and not a serious threat due to the ease of their detection.

Cavity virus

- **Cavity virus -** unlike traditional viruses the cavity virus does not attach itself to the end of the infected file but instead uses the empty spaces within the program files itself (that exists there for variety of reasons).

- This way the length of the program code is not being changed and the virus can more easily avoid detection.

- The injection of the virus in most cases is not impacting the functionality of the host file at all. The cavity viruses are quite rare though.

Task for You

- **Boot sector virus ????**
- **Polymorphic virus ????**
- **Armored virus ???**
- **Companion virus ???**

Types of Worms

- **Email worms**: spread through email messages, especially through those with attachments.
- **Internet worms**: spread directly over the internet by exploiting access to open ports or system vulnerabilities.
- **Network worms**: spread over open and unprotected network shares.
- **Multi-vector worms**: having two or more various spread capabilities.

Types of Trojans

- **Computer Trojans** or **Trojan horses** are named after the mythological Trojan horse from Trojan War, in which the Greeks give a giant wooden horse to their foes, the Trojans.

- As soon as Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their soldiers to capture Troy.

- Computer Trojan horse works in way that is very similar to such strategy - it is a type of malware software that masquerades itself as not-malicious even useful application but it will actually do damage to the host computer after its installation.

Types of Trojans

- Trojans *do not self-replicate* since its key difference to a virus and require often end user intervention to install itself - which happens in most scenarios where user is being tricked that the program he is installing is a legitimate one (this is very often connected with social engineering attacks on end users).

- One of the other common method is for the Trojan to be spammed as an email attachment or a link in an email.

- Another similar method has the Trojan arriving as a file or link in an instant messaging client.

- Trojans can be spread as well by means of **drive-by downloads** or **downloaded** and **dropped by other Trojans itself** or **legitimate programs that have been compromised**.

- The results of Trojan activities can vary greatly - starting from low invasive ones that only change **the wallpaper or desktop** icons through Trojans which open backdoors on the computer and allow other threats to infect the host or allow **a hacker remote access to the targeted computer system.**

- It is up to Trojans to cause serious damage on the host **by deleting files or destroying the data on the system** using various ways (like drive format or causing BSOD).

- Such Trojans are usually **stealthy and do not advertise** their presence on the computer.

Remote Access Trojans (RAT) *aka* **Backdoor. Trojan**

- This type of Trojan opens backdoor on the targeted system to allow the attacker remote access to the **system or even complete control over it.**

- This kind of Trojan is most widespread type and often has as well various other functions.

- It may be used as an **entry point** for **DOS attack** or for allowing worms or even other Trojans to the system.

Remote Access Trojans (RAT) *aka* **Backdoor. Trojan**

- A computer with a sophisticated backdoor program installed may also be referred to as a "**zombie" or a "bot".**

- A network of such bots may often be referred to as a **"botnet**“ or **Backdoor**.

- Trojans are generally created by **malware authors** who are organized and **aim to make money** out of their efforts.

- These types of Trojans can be highly sophisticated and can require more work to implement than some of the simpler malware seen on the Internet.

- **Trojan-DDoS -** This Trojan is **installed simultaneously** on a large number of computers in order to create a **zombie network (botnet) of machines** that can be used (as attackers) in a DDoS attack on a particular target.

- **Trojan-Proxy -** A proxy Trojan is a virus, which **hijacks and turns the host computer into a proxy server**, part of a botnet, from which an attacker can stage anonymous activities and attacks.

- **Trojan-FTP** – This Trojan is designed to **open FTP ports on the targeted machine** and allows a remote attacker access to the host.

- Furthermore, the attacker can also access as well network shares or connections to further extent more and other threats.

- **Destructive Trojan** – This is designed **to destroy or delete data**. It is much like a virus.

- **Security Software Disabler Trojan** – This is designed **to stop** security programs like **antivirus solutions, firewalls or IPS** either by disabling them or by killing the processes.

- This kind of Trojan functionality is **combined often with destructive Trojan** that can execute data deletion or corruption only after the security software is disabled.

- Security Software Disablers are entry Trojans that allow next level of attack on the targeted system.

- **Info Stealer (Data Sending/ Stealing Trojan) -** This Trojan is designed to provide an attacker with **confidential or sensitive information from compromised host** and send it to a predefined location (attacker).

- The stolen data comprise of **login details, passwords, PII, credit card information** etc.

- Data sending Trojans can also be designed to look for **specific information only or can be more generic** like Key-logger Trojans.

- Nowadays more than ever before attackers are concentrating on compromising end users for financial gain.

- The information stolen with use of Info stealer Trojan is often **sold on the black market**.

- Info stealers gather information by using several techniques.

- The most common techniques may include **log key strokes**, **screen shots** and **web cam images**, **monitoring internet activity often for specific financial websites**.

- The stolen information may be stored locally so that it can be **retrieved for later use or it can be sent to a remote location** where it can be accessed by an attacker.

- It is often encrypted before posting it to the malware author.

Keylogger Trojan

- **Keylogger Trojan** – This is a type of data-sending Trojan that is **recording every keystroke of the end user**.

- This kind of Trojan is used **specifically to steal sensitive information from targeted host** and send it back to attacker.

- For these Trojans, the goal is to collect as much **data as possible without any direct specification what the data will be.**

- **Trojan-PSW (Password Stealer)** – This is a type of data-sending Trojans designed specifically to **steal passwords from the targeted systems.**

- In its execution routine, the Trojan will very often first drop a keylogging component onto the infected machine.

- **Trojan-Banker** – A Trojan designed specifically to steal **online banking information to allow attacker** further access to bank account or credit card information.

- **Trojan-IM** – A type of data-sending Trojan designed specifically **to steal data or account information from instant messaging programs** like MSN, Skype etc.

- **Trojan-Game Thief** – A Trojan designed to **steal information about online gaming account.**

- **Trojan Mail Finder** – A Trojan used to **harvest any emails** found on the infected computer.

- The email list is then forwarded to the remote attacker.

- **Trojan-Dropper -** A Trojan-Dropper is a type of **trojan that drops** different type of standalone malware (trojans, worms, backdoors) to a system.

- It is usually an executable file that contains other files compressed inside its body.

- When a Trojan-Dropper is performed, it extracts these compressed files and saves them to a folder (usually a temporary one) on the computer.

- **Trojan.Downloader** – A Trojan that can download other malicious programs to the target computer.

- Very often combined with the functionality of Trojan-Dropper.
-
- Most downloaders that are encountered will attempt to download content from the internet rather than the local network.

- In order to successfully achieve its primary function, a downloader must run on a computer that is inadequately protected and connected to a network.

- **Trojan.FakeAV** – Trojan.FakeAV is a detection for Trojan horse programs that **intentionally misrepresent** the security status of a computer.

- These programs attempt to convince the user to purchase software in order to **remove non-existent malware** or security risks from the computer.

- The user is continually prompted to pay for the software using a credit card.

- Some programs employ tactics designed to annoy or disrupt the activities of the user until the software is purchased.

purchased.


Microsoft Internet Explorer
Attention! Your PC may not have privacy protection system. This may lead to irretrievable results.
Now your system will be scanned for privacy security risks.
Press OK to continue.
OK
Cancel


The page at http:// -protection.com says:
Warning! Your PC is at risk of virus and malware attack.
Your system requires immediate check!
System Security will perform a quick and free scan of your PC for viruses and malicious programs.
OK


Security Tool Warning
Security Tool has detected harmful software in your system.
We strongly recommended you to register Security Tool to
remove these threats immediately.

- This type of Trojan can be either targeted to extort money for "non-existing" threat removal or in other cases, the installation of the program itself injects other malware to the host machine.

- FakeAV applications can perform fake scans with variable results, but always detect at least one malicious object.

- They may as well drop files that are then ‘detected’. The FakeAV application is constantly updated with new interfaces so that they mimic the legitimate antivirus solutions and appear very professional to the end users.

- **Trojan-Spy** – this Trojan has a similar functionality to the Info stealer or Trojan-PSW and its purpose is to spy on the actions executed on the target host.

- These can include tracking data entered via keystrokes, collecting screenshots, listing active processes/ services on the host or stealing passwords.

- **Trojan-ArcBomb -**These Trojans are archives designed to freeze or trigger slow performance or to flood the disk with a large amount of “empty” data when an attempt is made to unpack the archived data.

- The so-called archive bombs pose a particular threat for file and mail servers when an automated processing system is used to process incoming data: an archive bomb can simply crash the server.

Trojan-Clicker or **Trojan-AD clicker** – A Trojan that continuously attempts to connect to specific websites in order to boost the visit counters on those sites.

More specific functionality of the Trojan can include generating traffic to pay-per-click web advertising campaigns in order to create or boost revenue.

Trojan-SMS – A Trojan used to send text messages from infected mobile devices to premium rate paid phone numbers.

- **Trojan-Ransom (Trojan-Ransomlock) aka Ransomware Trojan -** Trojan.Ransomlock is detection for Trojan horse programs that **lock the desktop of a compromised computer** making it unusable.

- The threat may arrive on the compromised computer by various means, such as visiting malicious sites, by opening untrusted links or advertisement banners, or by installing software from untrusted sources.

- Various functions on the compromised computer are modified, ranging from inhibiting access to the task manager to altering the master boot record (MBR) so that the operating system cannot be performed.

- These programs attempt to convince the user to pay money in order to have their computer unlocked and use a variety of different techniques in order to encourage the user to pay the ransom.

- **Cryptolock Trojan (Trojan.Cryptolocker)** – This is a new variation of Ransomware Trojan emerged in 2013, in a difference to a Ransomlock Trojan (**that only locks computer screen or some part of computer functionality**), the Cryptolock Trojan encrypts and locks individual files.

- While the Cryptolocker uses a common Trojan spreading techniques like spam email and social engineering in order to infect victims, the threat itself uses more sophisticated techniques likes public-key cryptography with strong RSA 2048 encryption.

Other security threats

- **Malware** refers to software viruses, spyware, adware, worms, trojans, ransomeware etc.
- They are designed to cause damage to a targeted computer or cause a certain degree of operational disruption.
- **Rootkit** are malicious software designed to hide certain processes or programs from detection.
- Usually acquires and maintains privileged system access while hiding its presence in the same time.
- It acts as a conduit by providing the attacker with a backdoor to a system.

- **Spyware** is a Software that monitors and collects information about a particular user, computer or organisation without user's knowledge.

- There are different types of spyware, namely system monitors, trojans (keyloggers, banker trojans, info stealers), adware, tracking cookies etc.

- **Tracking cookies** are a specific type of cookies that are distributed, shared and read across two or more unrelated websites for the purpose to gather information or potentially to present customized data to the user.

- **Riskware** is a term used to describe potentially dangerous software whose installation may pose a risk to the computer.

- **Adware** in general term is software generating or displaying certain advertisements to the user.

- This kind of adware is very common for freeware and shareware software and can analyze end user internet habits and then tailor the advertisements directly to users' interests.

- **Scareware** is a class of malware that includes both Ransomeware (Trojan.Ransom) and FakeAV software.

- Also well known, under the names of "Rogue Security Software" or "Misleading Software".

- This kind of software tricks user into belief that the computer is infected and offers paid solutions to clean the "fake" infection.

- **Spam** is the term used to describe unsolicited or unwanted electronic messages, especially advertisements. The most widely recognized form of spam is email spam.

- **Creepware** is a term used to describe activities like spying others through webcams (very often combined with capturing pictures), tracking online activities of others and listening to conversation over the computer's microphone and stealing passwords and other data.

- **Blended threat** defines an exploit that combines elements of multiple types of malware components.

- Usage of multiple attack vectors and payload types targets to increase the severity of the damage causes and as well the speed of spreading.

- Blended threat defines an exploit that combines elements of multiple types of malware components.

- Usage of multiple attack vectors and payload types targets to increase the severity of the damage causes and as well the speed of spreading.

Network Attacks

- **Network attack** is usually defined as an intrusion on the network infrastructure that will first analyse the environment and collect information in order to exploit the existing open ports or vulnerabilities.
- This may include unauthorized access to organisation resources.

Characteristics of network attacks:

- **Passive attacks**: They refer to attack where the purpose is only to learn and get some information from the system, but the system resources will not be altered or disabled in any way.

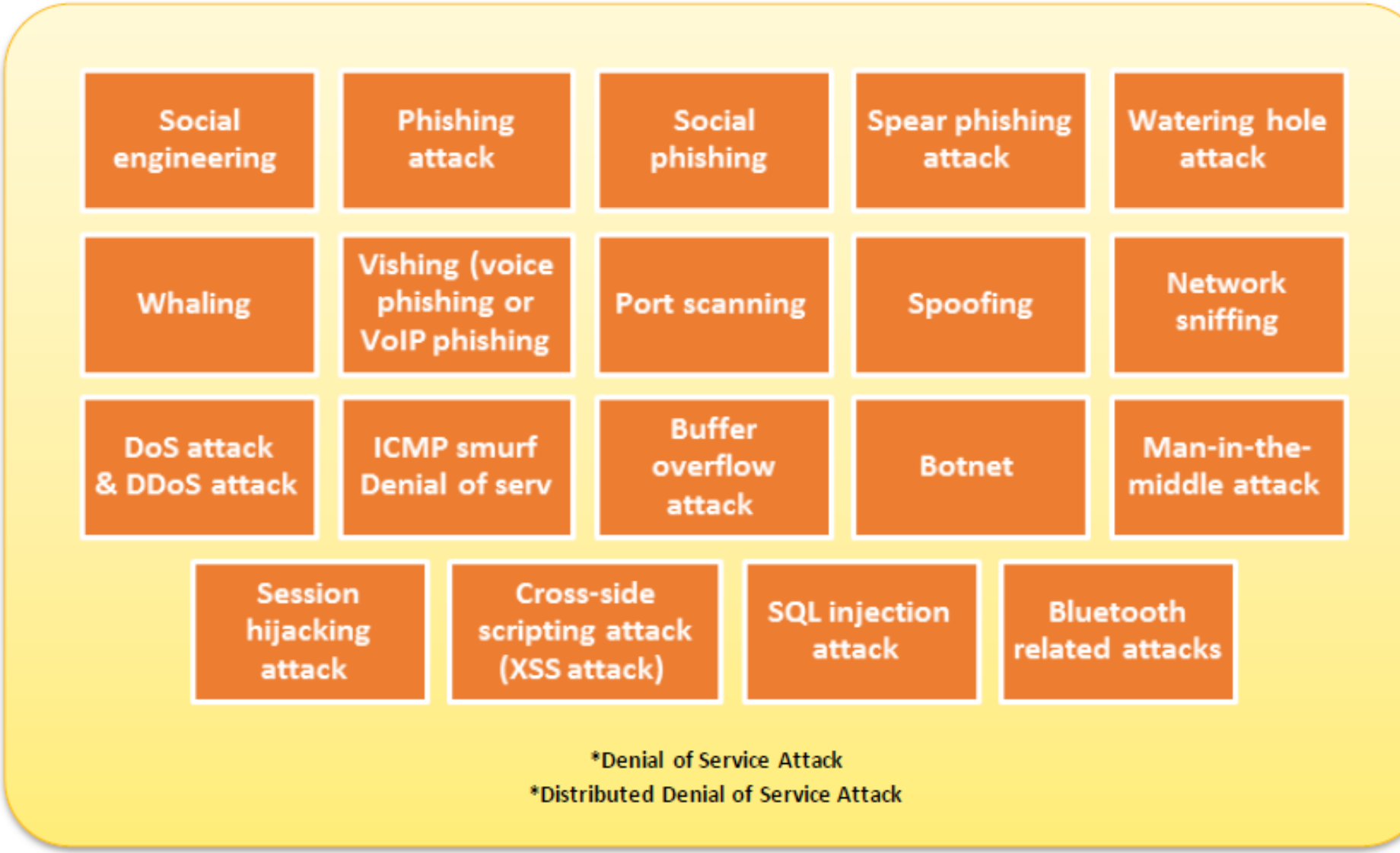
- **Active attacks:** In this type of network attack, the perpetrator accesses and either alters, disables or destroys resources or data.

Network Attacks

- **Outside attack:** When an attack is performed from outside of the organization by an unauthorized entity, it is referred to be an outside attack.

- **Inside attack:** If an attack is performed from within the company by an "insider" that already has certain access to the network it is considered to be an inside attack.

- **Others such as end users targeted attacks (like phishing or social engineering):** These attacks are not directly referred to as network attacks, but are important to know due to their widespread occurrences.


Social engineering
Phishing attack
Social phishing
Spear phishing attack
Watering hole attack
Whaling
Vishing (voice phishing or VoIP phishing
Port scanning
Spoofing
Network sniffing
DoS attack & DDoS attack
ICMP smurf Denial of serv
Buffer overflow attack
Botnet
Man-in-the-middle attack
Session hijacking attack
Cross-side scripting attack (XSS attack)
SQL injection attack
Bluetooth related attacks
*Denial of Service Attack
*Distributed Denial of Service Attack

Definition

- Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

Dear user, congratulations!

We want to thank you for being a loyal **Google India** user! Your IP address [redacted] has been randomly selected to receive a FREE **Apple iPhone X**.

From time to time we select a handful of Google users to give them the opportunity to receive valuable gifts from our partners and sponsors. This is our way of thanking you for choosing Google as your preferred search engine.

Today is your lucky day! You are one of the 10 randomly selected users who will receive this gift.

To receive your gift, you simply have to complete our short and anonymous survey. But hurry! There are only a few gifts available today!

How satisfied are you with Google?

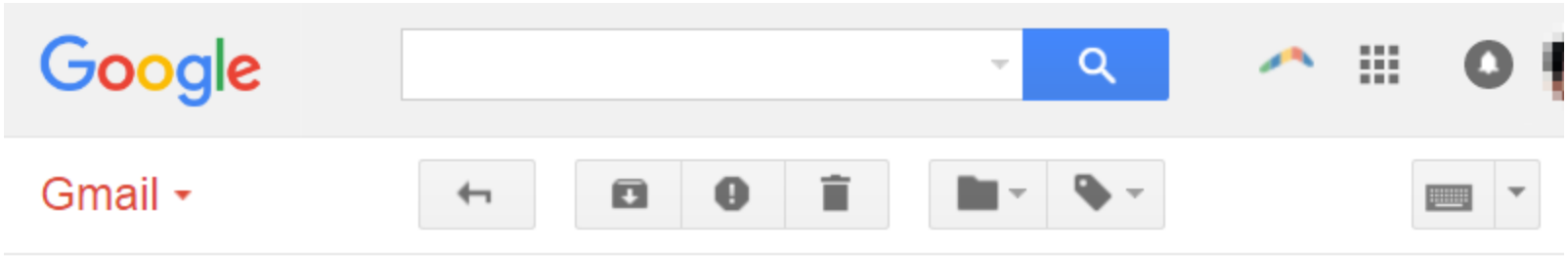
Very Satisfied | Satisfied | Unsatisfied

Phishing attack

- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

- It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

- The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.



Important: Your Password will expire in 1 day(s) Inbox x

MyUniversity 12:18 PM (50 minutes ago)

to me

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

MY UNIVERSITY

Thank you
MyUniversity Network Security Staff

Spear phishing Attack

- Spear phishing targets a specific person or enterprise, as opposed to random application users.

- It’s a more in-depth version of phishing that requires special knowledge about an organization, including its power structure.

TERAMIND

WATERING HOLE ATTACKS:

THREATS LYING IN WAIT

There's an advanced data security threat lurking, and experts have named it with the worst of analogies. A watering hole attack found in nature is where a diverse set of animals come together to drink unknowingly surrounded by predators. A fitting analogy for our cyber criminals that are targeting specific victims and infesting their systems with malware. This is how they do it:

1. FIND TARGET

Specific the target towards a particular company or industry.

2. GATHER DATA

Gather behavioral intel to understand the behavior of the target.

3. MALWARE INSTALLATION

Understand most frequently visited websites and attach malicious malware.

4. VULNERABILITY SCANS

Company user visits website and malicious code downloads in background. It runs vulnerability scan on the user's device.

5. EXPLOIT DELIVERY

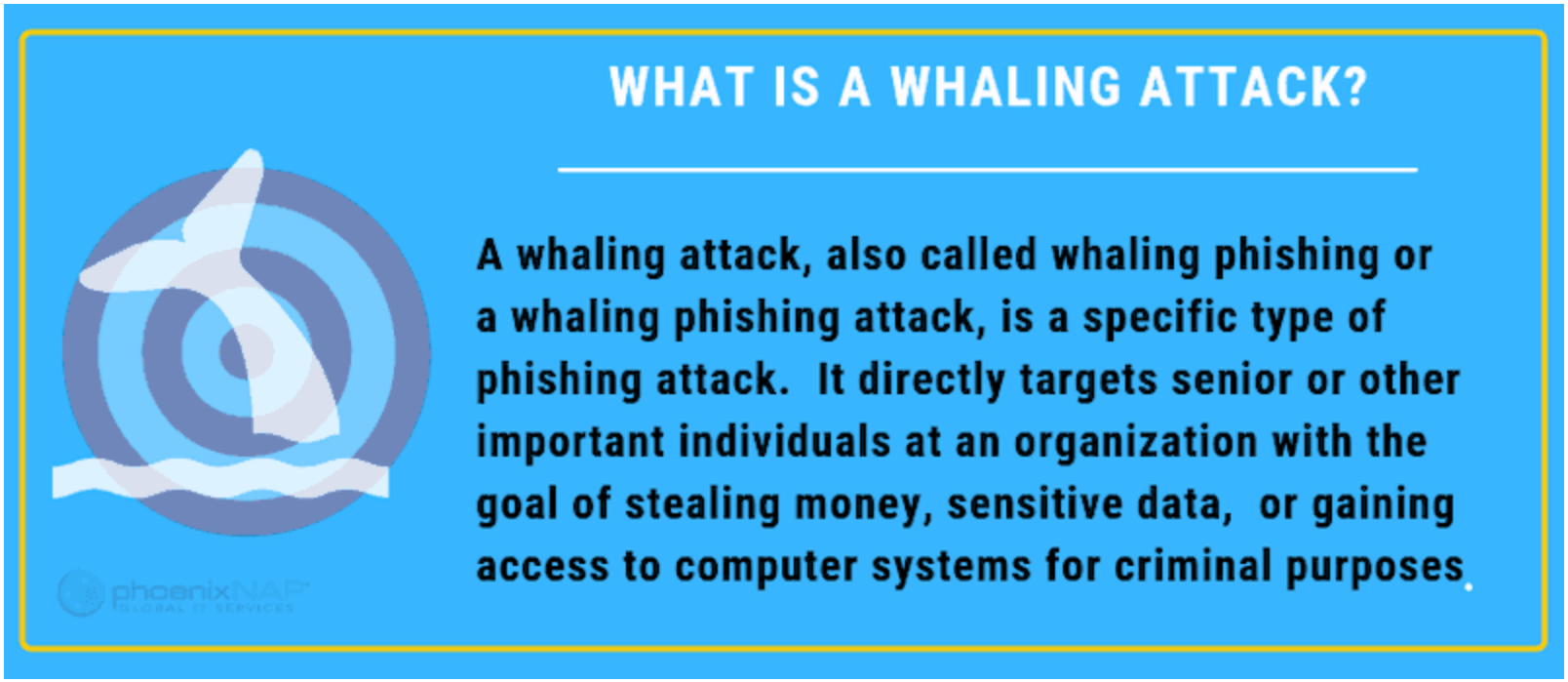
Vulnerabilities found, deliver malware into system.

6. SPREAD

Depending on the user's access, the malware can spread and affect more systems.

Watering hole attacks are becoming more targeted and successful. Many data safeguards can be established like consistent updates, user behavioral analytics and blocking customer analytic companies from tracking employee browsers. Teramind.co uses employee monitoring software to actively prevent information data breaches.

Whaling Attack



Whaling

Whaling emails are on the rise

From: CFO@companyO1.com
To: Bob@company01.com
Subject: Wire Transfer

Hi Bob, it's the CFO
I'm out of the office but could you make a wire transfer payment for me today?
Thanks

Example attack

$1.2 billion of losses reported to FBI in two years

Losses increased by $800m in last six months

Money involved traced to 108 countries

Source: FBI Internet Crime Complaint Center. $1.2 billion reported from October 2013 to August 2015. https://www.ic3.gov

mimecast

Common Vulnerabilities and Exposures (CVE)

- Common Vulnerabilities and Exposures (CVE) is a catalogue of known security threats.

- The catalogue is sponsored by the United States Department of Homeland Security (DHS), and threats are divided into two categories: vulnerabilities and exposures.

- According to the CVE website, a vulnerability is a mistake in software code that provides an attacker with direct access to a system or network.

Common Vulnerabilities and Exposures (CVE)

- For example, the vulnerability may allow an attacker to pose as a super user or system administrator who has full access privileges.

- An **exposure**, on the other hand, is defined as a mistake in software code or configuration that provides an attacker with indirect access to a system or network.

- For example, an exposure may allow an attacker to secretly gather customer information that could be sold.

Common Vulnerabilities and Exposures (CVE)

- The catalogue's main purpose is to **standardize the way** each known vulnerability or exposure is **identified**.

- This is important because standard IDs allow security administrators to quickly access technical information about a specific threat across multiple CVE-compatible information sources.

- CVE is sponsored by US-CERT, the DHS Office of Cybersecurity and Information Assurance (OCSIA).

Common Vulnerabilities and Exposures (CVE)

- MITRE, a not-for-profit organization that operates research and development centres sponsored by the U.S. federal government, maintains the CVE catalogue and public website.

- It also manages the CVE Compatibility Program, which promotes the use of standard CVE identifiers by authorized CVE Numbering Authorities (CNAs).

Vulnerability Enumeration

- Common Vulnerabilities and Exposures (CVE®) is a dictionary of common names (i.e. CVE Identifiers) for **publicly known information/cyber security vulnerabilities**.

- CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools.

- If a report from one of your security tools incorporates CVE identifiers, you may then **quickly and accurately access fix information** in one or more separate CVE compatible databases to remediate the problem.

Common Vulnerability Scoring System (CVSS)

- The Common Vulnerability Scoring System (CVSS) provides an **open framework** for communicating the characteristics and impacts of IT vulnerabilities.

- Its **quantitative model** ensures repeatable, accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores.

- Thus, CVSS is well suited as a **standard measurement system** for industries, organizations and governments that need accurate and consistent vulnerability impact scores.

Common Weakness Enumeration (CWE)

- The Common Weakness Enumeration Specification (CWE) provides a common language of discourse for discussing, finding and dealing with the causes of software security vulnerabilities as they are found in code, design or system architecture.

- Each individual CWE represents a **single vulnerability type.**

- CWEs are used as a **classification mechanism** that differentiates CVEs by the type of vulnerability they represent.

Key Elements of Information/cyber security

- **Network Security**
- **Application Security**
- **Communications Security**

Network Security

- Network security refers to **any activity designed to protect** your network.
- Specifically, these activities protect the **usability, reliability, integrity and safety** of your network and data.
- Effective network security targets a variety of threats and stops them from entering or spreading on your network.
- No single solution protects you from a variety of threats.
- You need multiple layers of security. If one fails, others still stand.
- Network security is accomplished through hardware and software.
- The software must be **constantly updated and managed** to protect you from emerging threats.
- Wireless networks, which by their nature, facilitate access to the radio, are more vulnerable than wired networks and need to encrypt communications to deal with sniffing and continuously checking the identity of the mobile nodes.

Network Security

- The **mobility factor** adds more challenges to security, namely **monitoring and maintenance of secure traffic transport** of mobile nodes.

- This concerns both **homogenous and heterogeneous mobility** (inter-technology), the latter requires homogenization of the security level of all networks visited by the mobile.

- From the terminal's side, it is important to protect its resources (battery, disk, CPU) against misuse and ensure the confidentiality of its data.

- In an **ad hoc or sensor network**, it becomes essential to ensure terminal's integrity as it plays a dual role of router and terminal.

Network Security

- The difficulty of designing security solutions that could address these challenges is
  - not only to ensure **robustness** faced with potential attacks or
  - to ensure that it does not **slow down communications**,
  - but also to optimize the **use of resources in terms of bandwidth, memory, battery,** etc.

- More importantly, in this open context the wireless network is to **ensure anonymity and privacy**, while allowing traceability for legal reasons.

- Indeed, the **growing need for traceability** is now necessary for the fight against criminal organizations and terrorists, but also to minimize the plundering of copyright.

Network Security

- It is therefore facing a dilemma of **providing a network support of free exchange of information** while c**ontrolling the content of the communication to avoid harmful content**.

- Actually, this concerns both wired and wireless networks.

- All these factors influence the **selection and implementation of security tools** that are guided by a prior risk assessment and security policy.

Network Security

- Finally, we are increasingly thinking about **trust models** in the design of secured systems, that **should offer higher level of trust than classical security mechanisms**, and it seems that future networks should implement **both models**: security and trust models.

- In fact, if communication nodes will be capable of building and maintaining a predefined trust level in the network, then the communication system will be trustable all the time, thus allowing a trusted and secure service deployment.

- However, such trust models are very difficult to design and the trust level is generally a biased concept presently. It is very similar to the human based trust model.

Network Security

- Note that succeeding in building such trust models will allow infrastructure based networks but especially **infrastructure-less or self-organized networks** such as ad hoc sensors to be trusted enough to deploy several applications.

- This will also have an impact on current business models where the economic model would have to change in order to include new players in the telecommunication value chain such as users offering their machines to build an infrastructure-less network.

- For example, in the context of ad hoc networks, we could imagine that ad hoc users become distributors of content or provide any other networked services, being a sort of service providers.

Network Security

- In this case, an appropriate charging and billing system needs to be designed.

- A network security system usually consists of many components. Ideally, all components work together, which minimizes maintenance and improves security.

Network security components often include:

- Anti-virus and anti-spyware
- Firewall to block unauthorized access to your network
- Intrusion Prevention Systems (IPS) to identify fast-spreading threats, such as zero-day or zero-hour attacks
- Virtual Private Networks (VPNs) to provide secure remote access Communication security

Application Security

- Application security (AppSec) is the use of software, hardware and procedural methods to **protect applications** from external threats.

- AppSec is the operational solution to the problem of software risk.

- AppSec helps identify, fix and prevent security vulnerabilities in any kind of software application irrespective of the function, language or platform.

Application Security

As a best practice, AppSec employs proactive and preventative methods to manage software risk, and align an organization's security investments with the reality of today's threats.

It has three distinct elements:

1) Measurable reduction of risk in existing applications

2) Prevention of introduction of new risks

3) Compliance with software security mandates

- AppSec as a discipline is also becoming more complex the variety of business software continues to proliferate.

Application Security

- Today's enterprise software comes from a variety of sources
  - in-house development teams,
  - commercial vendors,
  - outsourced solution providers, and
  - open source projects.

Application Security

- Software developers have an endless **choice of programming languages** to choose from – Java, .NET, C++, PHP and more.

- Applications can be **deployed** across myriad platforms– **installed to operate locally**, over virtual servers and networks, accessed as a service in the cloud or run on mobile devices.

- AppSec products must provide capabilities for **managing security risk** across all of these options as each of these **development and deployment** options can introduce security vulnerabilities.

Begin with software security testing to find and assess potential vulnerabilities:

- Follow **remediation** procedures to prioritize and fix them.
- **Train** developers on secure coding practices.
- **Leverage ongoing threat intelligence** to keep up-to-date.
- **Develop continuous methods** to secure applications throughout the **development life cycle.**
- Instantiate policies and procedures that in still good governance.

Application Security

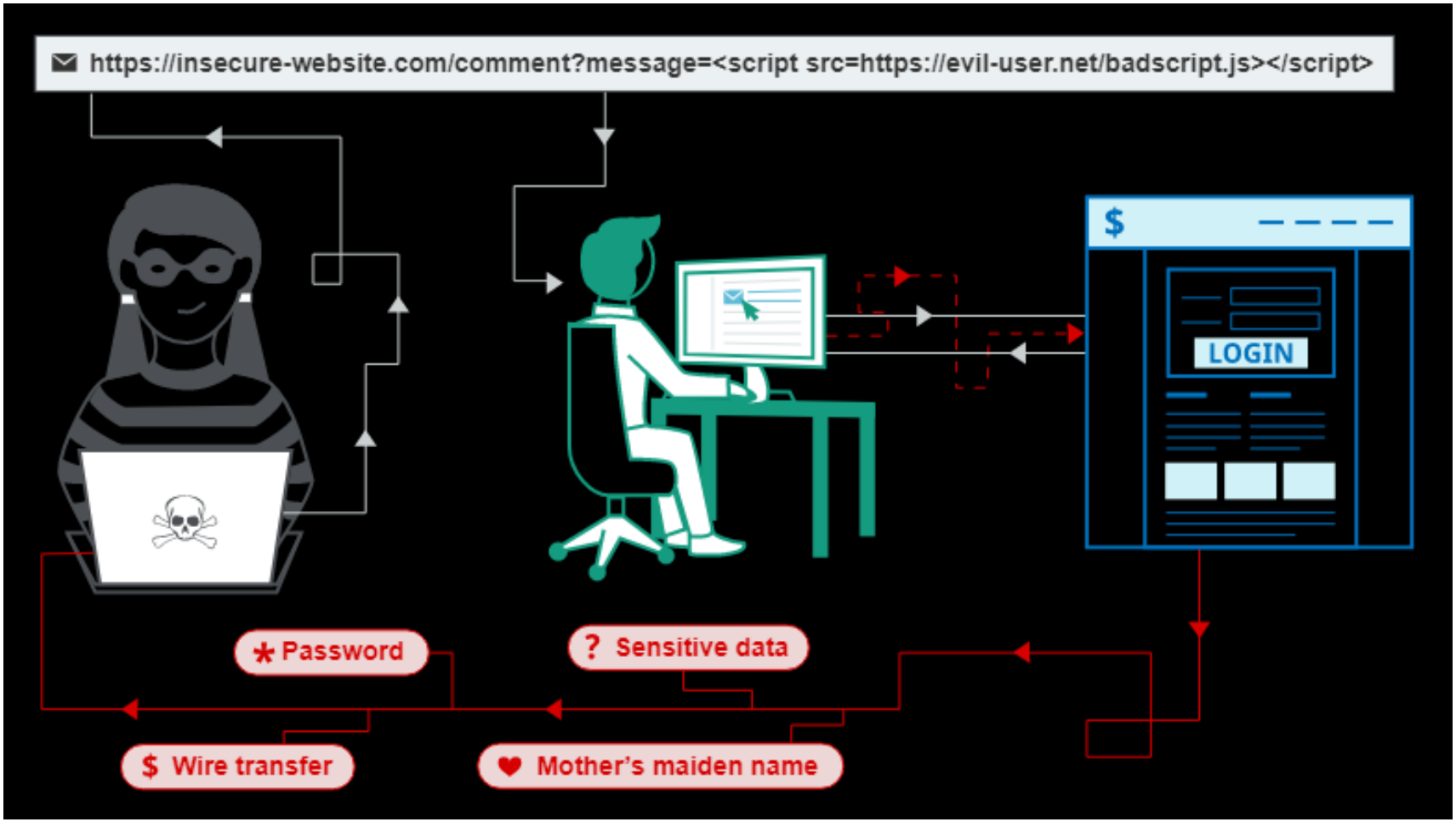
- Testing and remediation form the baseline response to insecure applications, but the **critical element** of a successful AppSec effort is **ongoing developer training.**

- **Security conscious development** teams write **bulletproof code**, and **avoid common errors**.

- For example, data input validation – the process of ensuring that a program operates with clean, correct and useful data.

- Neglecting this important step, and failing to build in standard input validation rules or “check routines” leaves the application open to common attacks such as cross-site scripting and SQL injection.

Cross Site Scripting



Cross-Site Scripting (XSS) attacks

- **Cross-Site Scripting** (**XSS**) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted **websites**.

- **XSS** attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side **script**, to a different end user.

Severity of Attack

- Depending on the severity of the attack, user accounts may be compromised, Trojan horse programs activated and page content modified, misleading users into willingly surrendering their private data.

- Finally, session cookies could be revealed, enabling a perpetrator to impersonate valid users and abuse their private accounts.

Two types of Cross-Site Scripting (XSS) attacks

- Cross site scripting attacks can be broken down into two types: stored and reflected.

- Stored XSS, also known as persistent XSS, is the more damaging of the two. It occurs when a malicious script is injected directly into a vulnerable web application.

- Reflected XSS involves the reflecting of a malicious script off of a web application, onto a user’s browser. The script is embedded into a link, and is only activated once that link is clicked on.

SQL injection

- SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.

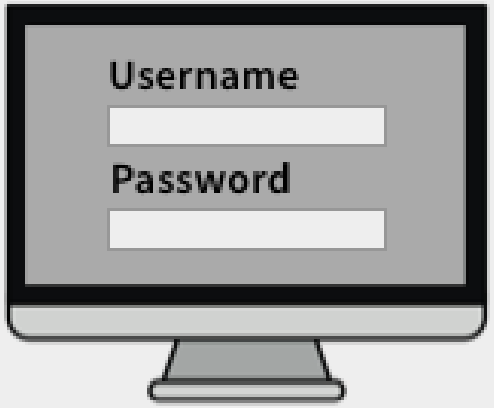
- It generally allows an attacker to view data that they are not normally able to retrieve.

- This might include data belonging to other users, or any other data that the application itself is able to access.

- In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

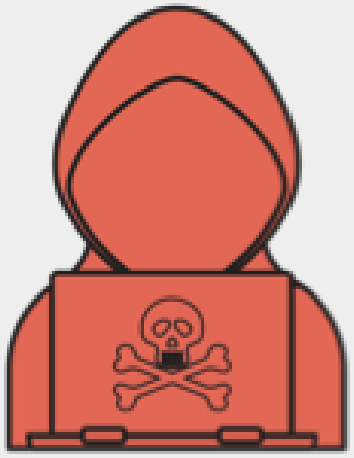
SQL Injection Attack (SQLi)

1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.



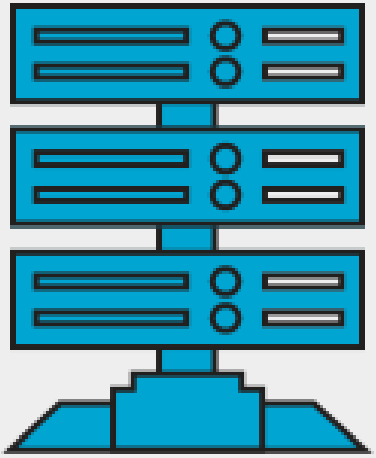
WEBSITE
INPUT FIELDS

2. Malicious SQL query is validated & command is executed by database.



HACKER

3. Hacker is granted access to view and alter records or potentially act as database administrator.



DATABASE

SQL injection examples

- Retrieving hidden data, where you can modify an SQL query to return additional results.
- Subverting application logic, where you can change a query to interfere with the application's logic.
- UNION attacks, where you can retrieve data from different database tables.
- Examining the database, where you can extract information about the version and structure of the database.
- Blind SQL injection, where the results of a query you control are not returned in the application's responses.

Application Security

- When undertaken correctly, Application Security is an orderly process of reducing the risks associated with developing and running business critical software.

- Properly managed, a good application security program will move your organization from a state of unmanaged risk and reactive security to effective, proactive risk mitigation.

Communications Security

- Communications Security (COMSEC) ensures the security of telecommunications confidentiality and integrity – the two Information Assurance (IA) pillars.

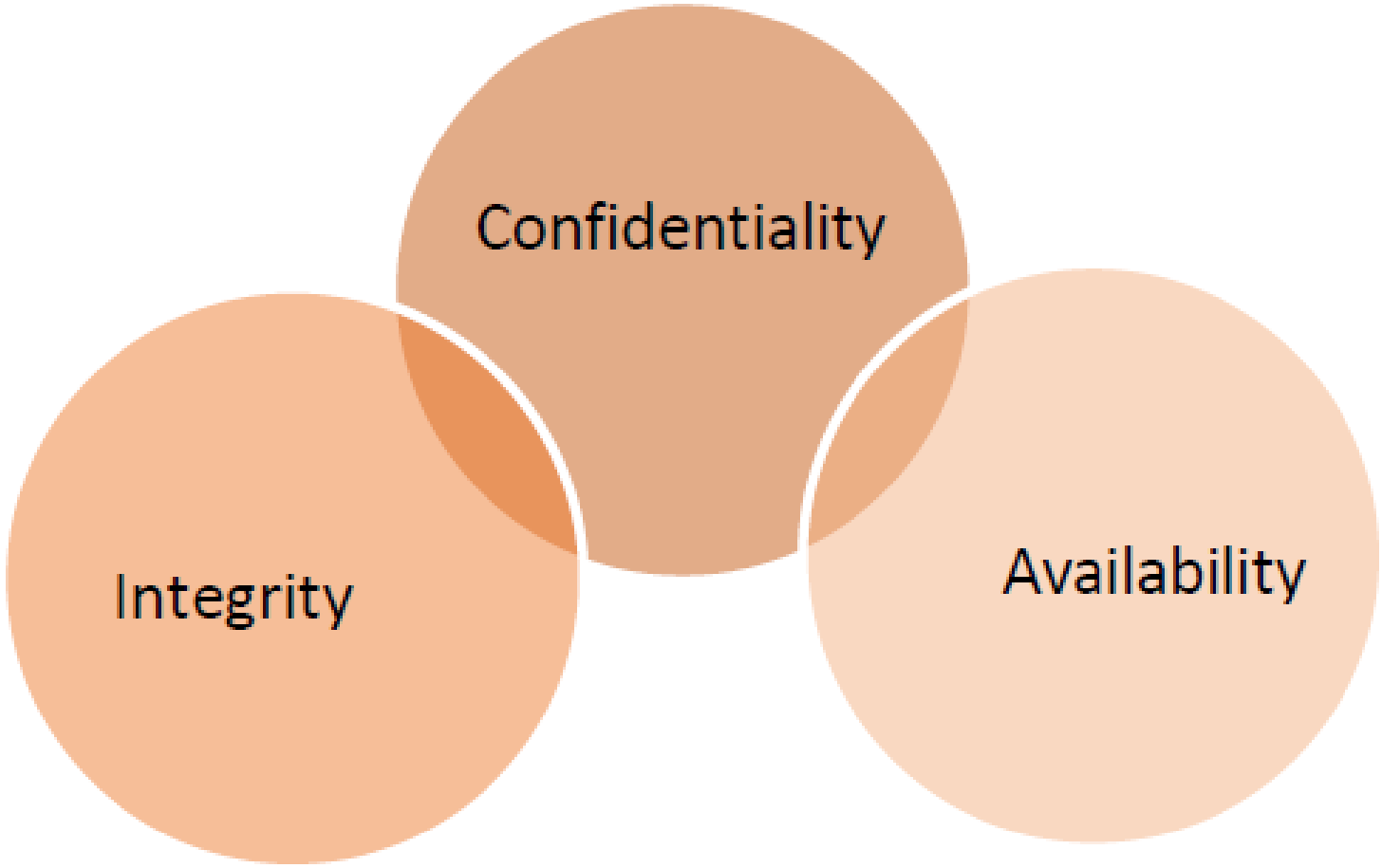
- Generally, COMSEC may refer to the security of any information that is transmitted, transferred or communicated.

- **There are five COMSEC security types:**

There are five COMSEC security types:

- **Crypto Security:** This **encrypts data**, rendering it unreadable until the data is decrypted.
- **Emission Security (EMSEC):** This prevents the release or capture of emanations from equipment, such as cryptographic equipment, thereby preventing unauthorized interception.
- **Physical Security:** This ensures the safety of, and prevents unauthorized access to, cryptographic information, documents and equipment.
- **Traffic-Flow Security:** This hides messages and message characteristics flowing on a network.
- **Transmission Security (TRANSEC):** This protects transmissions from unauthorized access, thereby preventing interruption and harm.

Principles and Concepts – Data Security



Information States

- Information has **three basic states**, at any given moment; information is being **transmitted**, **stored** or **processed**.

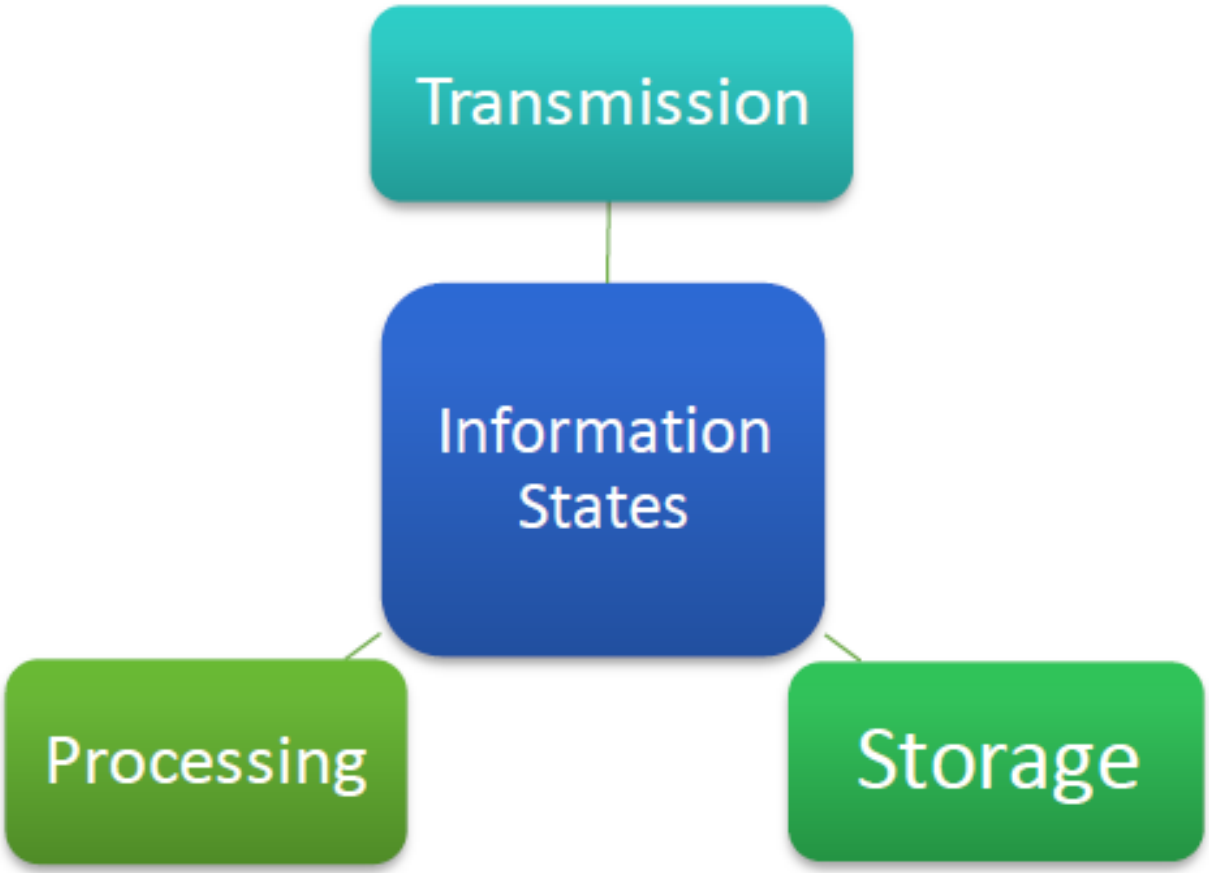
- The three states exist **irrespective of the media** in which information resides.

- Information systems security concerns itself with the maintenance of three critical characteristics of information: **confidentiality**, **integrity** and **availability**.

- These attributes of information represent the full spectrum of security concerns in an **automated environment**.

- They are applicable for any organization irrespective of its philosophical outlook on sharing information.

Information States



Prevention vs. detection

- Security efforts to assure confidentiality, integrity and availability can be divided into those oriented to prevention and those focused on detection.

- The latter aims to rapidly discover and correct for lapses that could not be (or at least were not) prevented.

- The balance between prevention and detection depends on the circumstances and the available security technologies.

Basic information/cyber security concepts

- Identification
- Authentication
- Authorization
- Confidentiality
- Integrity
- Availability
- Non-repudiation

Identification

- ***Identification*** is the first step in the ‘identify-authenticate-authorize’ sequence that is performed every day countless times by humans and computers alike when access to information or information processing resources are required.

- While particulars of identification systems differ depending on who or what is being identified, some intrinsic properties of identification apply regardless of these particular.

- Just three of these properties are the *scope*, *locality*, and *uniqueness* of IDs.

Identification

- Identification name spaces can be local or global in scope. To illustrate this concept, let’s refer to the familiar notation of email addresses.

- While many email accounts named *Gaurav* may exist around the world, an email address *Gaurav@company.com* unambiguously refers exactly to one such user in the company.com locality.

Authentication

- Authentication happens right after identification and before authorization.
- It verifies the authenticity of the identity declared at the identification stage.
- In other words, it is at the authentication stage that you prove you are indeed the person or the system you claim to be.
- The three methods of authentication are ***what you know, what you have and what you are.***
- Regardless of the particular authentication method used, the aim is to obtain reasonable assurance that the identity declared at the identification stage belongs to the party in communication.

Authentication

- It is important to note that *reasonable assurance* may mean **different degrees of assurance**, depending on the particular environment and application, and therefore may require different approaches to authentication.

- Authentication requirements of a national security – critical system naturally **differ from** authentication requirements of a small company.

- As different authentication methods **have different costs and properties as well as different returns on investment**, the choice of authentication method for a particular system or organization should be made after these factors have been carefully considered.

Authorization

- ***Authorization*** is the process of ensuring that a user has sufficient rights to perform the requested operation, and preventing those without sufficient rights from doing the same.

- After declaring identity at the identification stage and proving it at the authentication stage, users are assigned a set of authorizations (also referred to as **rights, privileges or permissions**) that define what they can do on the system.

- These authorizations are most commonly defined by **the system's security policy** and are set by the security or **system administrator**.

- These privileges may range from the extremes of **"permit nothing"** to **"permit everything**" and include anything in between.

Confidentiality

- ***Confidentiality*** means **persons authorized have access to receive or use information, documents etc**.

- Unauthorized access to confidential information may have devastating consequences, not only in national security applications, but also in commerce and industry.

- Main mechanisms of protection of confidentiality in information systems are **cryptography and access controls.**

- Examples of threats to confidentiality **are malware, intruders, social engineering, insecure networks and poorly administered systems.**

Integrity

- ***Integrity*** is concerned with the trustworthiness, origin, completeness and correctness of information as well as the prevention of improper or unauthorized modification of information.

- Integrity in the information/cyber security context refers not only to integrity of information itself but also to the origin integrity i.e. integrity of the source of information.

- Integrity protection mechanisms may be grouped into two broad types: **preventive mechanisms**, such as access controls that prevent unauthorized modification of information, and

Integrity

- **Detective mechanisms**, which are intended to detect unauthorized modifications when preventive mechanisms have failed.

- Controls that protect integrity include principles of least privilege, separation and rotation of duties.

Availability

- Attacks against availability are known as Denial Of Service (DoS) attacks.

- **Natural and manmade disasters** obviously may also affect availability as well as confidentiality and integrity of information though their frequency and severity greatly differ.

- Natural disasters are infrequent but severe, whereas human errors are frequent but usually not as severe as natural disasters.

- In cases, business continuity and disaster recovery planning (which at the very least includes regular and reliable backups) is intended to minimize losses.

Non-repudiation

- A digital signature owner, who may like to repudiate a transaction maliciously, may always claim that his/ her digital signature key was stolen by someone who actually signed the digital transaction in question, thus repudiating the transaction.

Types of Controls

- Central to information/cyber security is the concept of controls, which may be categorized by their functionality (preventive, detective, corrective, deterrent, recovery and compensating) and plane of application (physical, administrative or technical) as follows

By functionality:

- **Preventive controls :** Preventive controls are the first controls met by an adversary. These try to prevent security violations and enforce access control.
- Like other controls, these may be physical, administrative or technical.
- Doors, security procedures and authentication requirements are examples of physical, administrative and technical preventive controls respectively.

Detective controls

- Detective controls are in place to detect security violations and alert the defenders.

- They come into play when preventive controls have failed or have been circumvented and are no less crucial than detective controls.

- Detective controls include cryptographic checksums, file integrity checkers, audit trails and logs and similar mechanisms.

Corrective controls

- Corrective controls try to correct the situation after a security violation has occurred.

- Although a violation occurred, but the data remains secure, so it makes sense to try and fix the situation.

- Corrective controls vary widely, depending on the area being targeted, and they may be technical or administrative in nature.

Deterrent controls

- Deterrent controls are intended to discourage potential attackers.

- Examples of deterrent controls include notices of monitoring and logging as well as the visible practice of sound information/cyber security management.

Recovery controls

- Recovery controls are somewhat like corrective controls, but they are applied in more serious situations to recover from security violations and restore information and information processing resources.

- Recovery controls may include disaster recovery and business continuity mechanisms, backup systems and data, emergency key management arrangements and similar controls.

Compensating controls

- Compensating controls are intended to be alternative arrangements for other controls when the original controls have failed or cannot be used.

- When a second set of controls addresses the same threats that are addressed by another set of controls, it acts as a compensating control

By plane of application

- **Physical controls** include doors, secure facilities, fire extinguishers, flood protection and air conditioning.

- **Administrative controls** are the organization's policies, procedures and guidelines intended to facilitate information/cyber security.

- **Technical controls** are the various technical measures, such as firewalls, authentication systems intrusion detection systems and file encryption among others.