1.1 Networking Fundamentals

A network connects two or more computers to communicate with each other or for the exchange of information among the systems. Networking is sharing of the resources within a network.

In basic communication, there are three components involved : the sender, the receiver, and the media. In the case of two people communicating with each other face to face, within a short distance, the media could be just air.

As shown in below Fig. 1.1.1, communication is completed only when the sender and receiver understand each other and are able to understand the information.

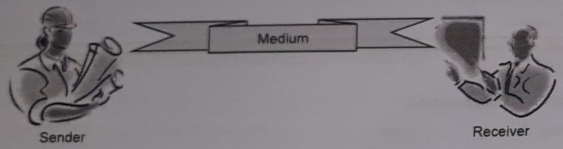

Fig. 1.1.1 Communication partners

In order to understand the information clearly that is being exchanged between the sender and the receiver, the communication "protocol" could be common a "language."

Protocol is a set of rules defined by the communication channel in order to comprehend the information that is being exchanged and in normal human communication, it is a common language understood by both the parties.

1.1.1 Steps in Communication Process

Suppose the sender understands a different language and the receiver understands a different language. For example say the sender understands Gujarati and the receiver understands Marathi. Assume that both have to exchange information, the media is Facsimile (FAX) in Gujarat and Telegraph in Maharashtra.

This communication has increased the complexity as both sender and receiver do not have a common language and there is no common media. The communication needs translators who understand both the languages or two translators - one who understands the sender's language (e.g., Gujarati) and another common language (e.g., Hindi/English), another who understands a common language (e.g., Hindi/English) and the receiver's language (e.g., Marathi). These translators translate to the senders and receivers. A media translator transfers facsimile information on to the telegraphic information and vice versa.

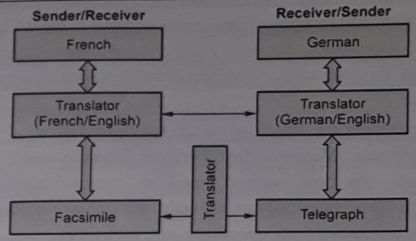

Fig. 1.1.2 Layered communication architecture

As shown in the above Fig. 1.1.2, this type of communication is called layered communication. Through the different layer, communication is achieved, each layer has a specific task and tasks are broken down into simple and specific tasks.

Though both sender and receiver do not have a common language, they are still able to interoperate with the help of layered communication.

1.1.2 Computer Networks and Communication Over the Computer Network

In the case of data communication, computer devices are connected logically to each other and data is transmitted from one computer system to another or from one device to another device as shown in below Fig. 1.1.3.

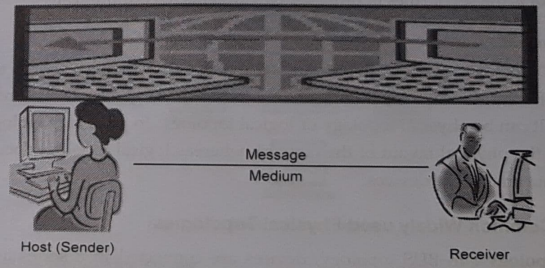

Fig. 1.1.3 Computer communication

A **network** connects two or more computers to communicate with each other or for the exchange of information among the systems. **Networking** is sharing of resources within the network.

Data communication and computer networking go hand in hand. Data communication is the exchange of information across a medium and networking is connecting two devices to facilitate the exchange of information from one system to another in a connected network.

When computer devices are connected in a network for communication, it consists of the following components : Message, Host, Receiver, Medium and Protocol. When these network components (the host, receiver, medium, protocol and other devices) are connected with each other, physically or logically, the primary consideration is whether the systems are able to communicate effectively with each other.

Use of appropriate systems or network components with deployment of appropriate protocols ensures effective communication among the systems.

1.1.3 Network and its Components

The network components

- **Message** is the information one computer system is sending to another.
- **Host** is the sender of message.
- **Receiver** is one who is receiving the information.
- **Medium** is the channel of communication. It can be copper wire, optical fiber or wireless.
- **Protocol** is the set of rules in order for two systems to communicate.

Topology Concept

Network "topology" refers to the layout of the network. Topology defines the method of placing different nodes in a network and how the data is getting transferred between these nodes. It can be physical topology or logical topology. In physical topology, there is emphasis on the physical layout of the network whereas logical topology focuses on the transfer of data among the devices.

1.1.4 The Common Widely used Physical Topologies

- **Bus topology :** In BUS topology, devices are connected in a series as shown in below Fig. 1.1.4 In this topology, all the devices are connected sequentially to the same line (as shown in the Fig. 1.1.4). This is a simple and low-cost solution but the failure of any single device or damage to the medium can bring down the entire network.

- **Ring topology :** All the devices are connected sequentially in the form of a ring (as shown in below Fig. 1.1.4). This topology is similar to the linear bus except that the ring ends at the start of the node. The disadvantage of the ring topology is, if any one of the devices breaks, the entire ring breaks.
- **Star or Y topology :** All the devices are connected through a central hub (as shown in below Fig. 1.1.4). Unlike in the previous topologies, failure of a single device does not necessarily bring down the entire network unless the central hub device is down. This is the most popular topology currently deployed by many organizations because it is simple to build, connect, and it is simple to add and remove devices to/from the network.

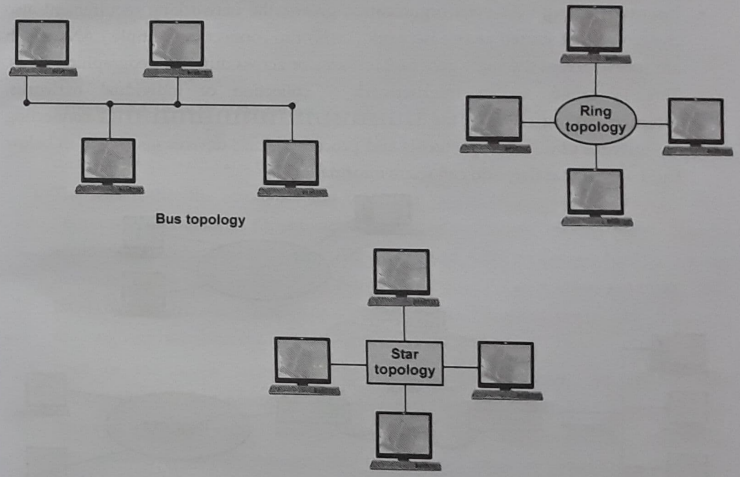

Fig. 1.1.4 : Network topologies

1.1.5 Computer Networks Types

- **Local Area Network (LAN) :** A Local Area Network is a network that is confined to a relatively small geographical area such as a school or an office building and occasionally a group of nearby buildings. LAN connects a relatively small number of systems within the same organization. The most common LAN protocol is ethernet.

- **Wide Area Network (WAN) :** Wide Area Network (WAN) connects two or more LANs which are geographically apart. For example, an organization may have two different offices in two different places or countries and they are connected together to form a WAN. WAN connections comprises of several devices including multiplexers, bridges, and routers. WAN link can be a private dedicated link or a public link.
- **Metropolitan Area Network (MAN) :** Metropolitan Area Networks (MAN) is a network of connected systems within the same metropolitan city. A MAN is larger than a LAN but smaller than a WAN. For practical reasons, a MAN is optimized for a large geographical area, and can connect two types of networks - LAN and WAN.
- **Internetworking :** As your organization grows, the networking requirement also changes. What started as one network (LAN) can connect to multiple LANs which are spread across the same geographical area or across different geographical areas. This is called as an internetwork – collection of individual networks. **Internetworking** refers to the 11111111111111111111111111111111111 connecting of networks of different protocols and procedures and devices (as shown in below Fig. 1.1.5) so that they still can share information.

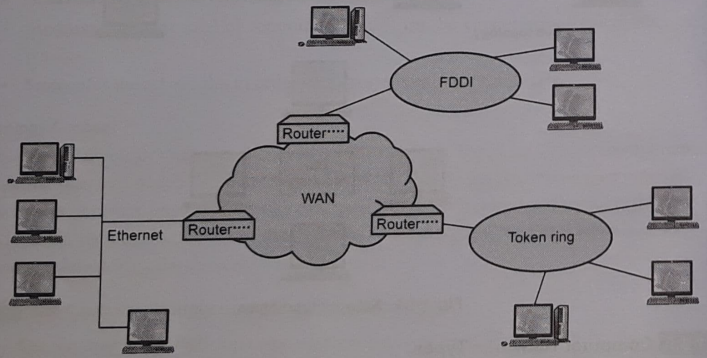

Fig. 1.1.5 : Internetworking

1.1.6 Network Protocols

A protocol, in computer communications terms, is a set of rules that governs the communication between two or more computers connected on a network. It is a common language for different vendor devices to talk to each other on a network.

In order to meet the challenges of multi-vendor devices on a network and to break the complexity of computer communications, there are two types of networking models that are developed based on the layered protocol approach. These models are the OSI and the TCP/IP. OSI is a seven-layer model whereas TCP/IP is a four-layer model which overlaps several layers of OSI functionality.

1.1.6.1 OSI (Open Systems Interconnection) Reference Model

1. ISO, the International Organization for Standardization, is a global body of representatives from over 150 countries. The ISO is a nongovernmental organization that bridges the gap between the government, public and private organizations.
2. In 1982, the ISO and the International Telecommunication Union Standardization Sector (ITU-T) developed a vendor-neutral, Open Systems Interconnection (OSI) protocol for devices communicating in a multi-vendor network environment. The OSI reference model divides the complex computer communication into seven distinct layers, with each layer having its own specific functions and protocols.
3. The reason that the acronyms and name are not matching is explained by ISO - "Because 'International Organization for Standardization' would have different acronyms in different languages (IOS in English, OIN in French for *Organisation internationale de normalisation*), our founders decided to give it the short form ISO. ISO is derived from the Greek isos, meaning equal. Whatever the country, whatever the language, the short form of our name is always ISO."
4. Each of the seven layers is responsible for a particular function of data communication. For example, one layer may be responsible for routing the data between devices, while another layer may be responsible for establishing connection between the devices. The upper layers focus on presenting information to the user at the application level whereas the lower layers focus on transporting the information across the network without any data loss. Each layer is functionally independent of the other layers. In the OSI reference model, each of the layers extends services to the layer directly above it and is given services from the layer directly below it. Hence all the seven layers together bring about the communication between the devices in a network. Below figure describes the seven layers, and the functions that are performed by each layer.

7	**Application layer** Message format
6	**Presentation layer** Encryption, Compression
5	**Session layer** Authentication, Permissions, Session management
4	**Transport layer** End-to-end guaranteed delivery
3	**Network layer** Delivering data over internetworking (Routing, Switching)
2	**Data link layer** Media access, Flow control
1	**Physical layer** Bit stream on physical media

Fig. 1.1.6 : OSI seven layer reference model

Below is the detail description of each layer working.

1. **Layer 7 - Application layer :** The application layer has the responsibility of providing application services to the network applications such as e-mail, web, remote connection, file transfers and database access. Some of the other functions that are performed at this layer include user authentication and data encryption. Application examples include *WWW browsers, Hypertext Transfer Protocol (HTTP), Simple Network Management Protocol (SNMP), Telnet, File Transfer Protocol (FTP), Domain Name System (DNS), Internet Message Access Control (ICMP), and Dynamic Host Configuration Protocol (DHCP).*
2. **Layer 6 - Presentation layer :** Presentation layer's responsibility includes presenting the data to the upper layers. This layer transforms the data into a required format that can be accepted by the applications in the application layer. For example, some Web browsers accept jpeg, some accept gif, some accept ASCII, and so on. This layer also manages techniques such as data compression and data encryption. Examples include *ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, and MIDI.*
3. **Layer 5 - Session layer :** This layer manages the establishment, the usage, and the ending of the connections/sessions between the devices. This layer performs the function of establishing sessions between the devices, how long the sessions should be, which side will transmit, when to transmit and how long to transmit. Examples include RPC, SQL and NetBios.

4. **Layer 4 - Transport layer :** This layer's responsibility is to ensure that the delivery of data from one end point to another indeed gets completed without any errors. This layer implements error checking, recovery of lost packets to ensure the completeness of data transfer and flow control. Some examples include Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Sequenced Packet Exchange (SPX).
5. **Layer 3 - Network layer :** Network layer is responsible for routing of the data within the network. It is responsible for finding the shortest path from source to destination and route the packet through the intermediate devices such as router(s) or switch(es). Examples include Internet Protocol (IP), Internetwork Packet Exchange (IPX) and AppleTalk.
6. **Layer 2 - Data link layer :** This layer consists of two sub-layers : Media Access Control (MAC) and Logical Link Layer (LLC). The Media Access Control Layer is responsible for taking the packets from the above layers and putting them onto the media in the form of bits. The media can be copper (wired), optical fiber, or wireless. LLC connects to the upper network layer. The function of the LLC layer is to control the frame synchronization, flow control of data and error checking of the frames (Cyclic Redundancy Check). Examples include *IEEE 802.5/ 802.2, IEEE 802.3/802.2, Frame Relay, Asynchronous Transfer Mode (ATM), and Integrated Services Digital Network (ISDN).*
7. **Layer 1 - Physical layer :** This layer is responsible for transmitting bits (0s and 1s) from one device to another device over a physical media. The media could be wire, wireless or optical fiber. Both the data link layer and the Physical Layer functions are implemented at the hardware level attached to the computer as a peripheral device known as the Network Interface Card (NIC).

1.1.6.2 TCP/IP Model

Earlier the Department of Defense (DOD), as a part of research project, developed the ARPAnet protocol to connect devices in a network of networks (the "Internet"). Modification of this protocol for the public is what we know today as TCP/IP – Transmission Control Protocol (TCP) and Internet Protocol (IP). TCP/IP is made up of the following four layers :

1. **Application layer :** This layer combines the application, presentation, and session layer functionalities of the OSI reference model. The function of this layer is to hand over the data received from the bottom layer to the application and to make sure the application is able to interpret the data that it has received from the other network device.

2. **Transmission Control Protocol (TCP) layer :** The function of this layer is to deliver data from the client to the server without errors or loss. Data can be lost during the transmission but TCP ensures that the data is not lost and triggers retransmission process until the data is correctly and completely received by the destination device. This layer overlaps the functionality of transport layer of OSI reference model. In this layer, the data received from the application is broken down into smaller "chunks" called segments.
3. **Internet Protocol (IP) layer :** This layer is responsible for moving the data from one node to another node. IP forwards the segments received from the TCP, referred to as packets, to the destination based on the IP address. This layer's function is very similar to the network layer function of the OSI reference model and implements various routing protocols such as Remote Imaging Protocol (RIP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP).
4. **Network Access Layer/Physical layer :** It combines the functions of the Data Link and the Physical Layers of the OSI reference model. The network access layer is responsible for creating data 'frames' for transmitting and receiving data from the physical layer. This function is implemented by a hardware and software Network Interface Card (NIC), an adapter connected to the computer through physical wires or optical fiber cables. There are several protocols implemented in this layer: Ethernet, Gigabit Ethernet, ATM, ISDN, and frame relay. It can support copper or optical interface.

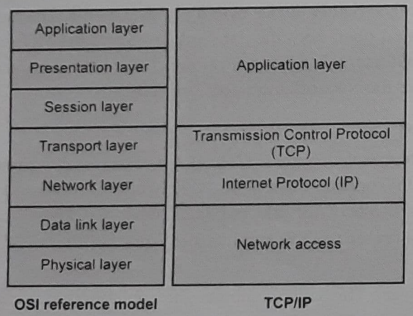

Fig. 1.1.7 : Illustrates the relationship between the OSI seven layers and TCP/IP

1.1.6.3 Comparison between OSI and TCP/IP Models

Each layer provides a distinct function and works with its upper layer and lower layer. Each layer "encapsulates" its function and passes on to the next layer while transmitting the data. When the data is received from lower layers, each layer peels off its encapsulation to perform its function. For the complete data transfer, functions of all the layers are equally important and all the layers have to work together. Layered architecture breaks the network communication into simpler components thus aiding easy design, development, and troubleshooting. With the layered architecture, each layer's functions can be developed by a different vendor who needs to adhere to the standards specified by the OSI reference model. The OSI model ensures different types of network devices built by different manufacturers such as routers, switches, hubs, and adapters, are able to interoperate within the network.

The (Internet Engineering Task Force) IETF is an international community consisting of network designers, equipment manufacturers, internet operators, and researchers who maintain the Internet protocol and the smooth operation of the Internet. RFC 1122 explains the details of host-to-host communication. RFC 791 describes IP and RFC 793 describes TCP architecture.

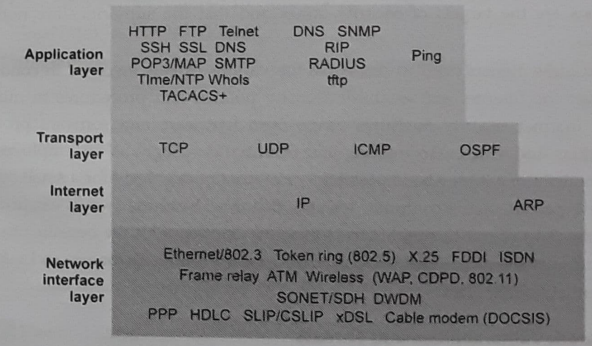

Fig. 1.1.8 : TCP/IP and its functions

Above Fig. 1.1.8 shows the TCP/IP protocol architecture and shows some of the major applications of each layer in respective layer.

1.2 Internet Security

Internet security is a broad term that refers to the various steps individuals and companies take to protect computers or computer networks that are connected to the Internet. One of the basic truths behind Internet security is that the Internet itself is not a secure environment.

The Internet was originally conceived as an open, loosely linked computer network that would facilitate the free exchange of ideas and information. Data sent over the Internet - from personal e-mail messages to online shopping orders - travel through an ever-changing series of computers and network links. As a result, unscrupulous hackers and scam artists have ample opportunities to intercept and change the information. It would be virtually impossible to secure every computer connected to the Internet around the world, so there will likely always be weak links in the chain of data exchange.

Due to the growth in Internet use, the number of computer security breaches experienced by businesses has increased rapidly in recent years. At one time, 80 percent of security breaches came from inside the company. But this situation has changed as businesses have connected to the Internet, making their computer networks more vulnerable to access from outside troublemakers or industry spies. Many a times big organizations are the targets of security attack and that the authorities are not made aware of this.

Small business owners need to recognize the various threats involved in conducting business over the Internet and establish security policies and procedures to minimize their risks. Internet security measures range from hardware and software protection against hackers and viruses, to training and information programs for employees and system administrators. It may be impossible - or at least impractical - for a small business to achieve 100 percent secure computer systems. But small business owners can find ways to balance the risks of conducting business over the Internet with the benefits of speedy information transfer between the company and its employees, customers and suppliers and all potential stakeholders.

1.2.1 Network Vulnerabilities and Threats

With the advancement in computing, networking, and technology, the world is becoming more and more connected. Internet connects millions of computers and most of the geographies of this world.

The Internet is a network of networks and consists of billions of users across private, public, university and government networks sharing information across the networks.

The Internet uses TCP/IP protocol and the underlying physical media can be wire, optical or wireless technologies.

The Internet serves an extensive range of applications, starting with e-mail, the World Wide Web (www), and social networks. Each application may use one or more protocols. There is a large amount of personal, commercial, business, government, and military information being shared on the Internet.

There are billions of users, both good and bad, accessing the Internet. The bad guys, known as hackers and such other persons with malicious intent are a concern.

With so many computers, networking devices, protocols, and applications on the network, it has become a serious threat to information security. Any application, network device or protocol can be vulnerable.

The internet is crawling with people from all over the world who are continuously trying to test the security of various systems and networks. Some are simply testing for fun and others are fuelled by treacherous motives of stealing or revenge.

A **threat** is an event that can occur by taking advantage of any vulnerabilities that exist in the network.

1.2.2 Common Terms Related to Network Security - Vulnerability, Threat, Attack

1. **Vulnerability -** An inherent weakness in the network, and network device. It could be hardware or software or both. Possible vulnerabilities could include routers, switches, servers, and security devices themselves.
2. **Threat -** A threat is what can go wrong because of the exploit of the vulnerabilities or attack on the assets, such as data theft or unauthorized modification of the data.
3. **Attack -** An attack is an unauthorized action with the intent to cause damage or hinder or breach security of a network. An attack is launched by intruders to damage the network and network resources such as end-point devices, servers or desktops which are vulnerable.

1.2.2.1 Vulnerabilities

One of the following three types of vulnerabilities or weaknesses can exist in any network,

- Security policy weakness
- Technology weakness
- Configuration weakness

1. Security policy weaknesses

Every organization should have security policies (An information technology security policy identifies the rules and procedures for all individuals accessing and using an organization's IT assets and resources) defined. However, the network can pose a security threat if the users do not follow the organizational security policy. Table 1.2.1 below summarizes some of the common security policy weaknesses.

Weakness	Possible problems
No written security policy	No enforcement of security policy across the organization leading to security incidents. Because of ignorance, mistakes may happen which can compromise the security. Intentional malicious acts also can be disguised as acts of ignorance. Unauthorized installations leading to theft of information; unauthorized modifications to the information.
No policy for hardware and software installations or updates	Unapproved modifications leading to unstable, attack prone network; ultimately leading to network crash. Unauthorized installations leading to malware infection. Intentional misuse of the network for personal gain.
Lack of disaster recovery and business continuity plans	Confusion during disaster. Disasters may not be effectively and efficiently handled leading to reputation loss, business loss, or customer loss.
No incident response team	Not able to handle security incidents / crisis, sometimes further complicating the situation rather than solving the problem.
No policy on usage of official assets	Misuse of official assets. Reputation Loss. Productivity loss. Can lead to malware infection.
No policy on teleworking or working from home	Use of personal machines to connect to the network leading to the theft of data or infection of the office network

Table 1.2.1 Common security policy weaknesses

2. Technology weaknesses

Protocols are standard set of rules created to specify how an application should communicate. All connection oriented protocols have a state. Each state triggers certain events at certain time. Each state can be part of the connection, for example, a server waiting for response from a client or the transition between the close of connections. Specifications are not always complete, they are a good starting point and they could have limitations. Not all the applications are created by taking care of all the points mentioned in the specification. Such weaknesses in the protocol can be exploited.

All data traffic on the network is not malicious. However, traffic is allowed or denied by the security policies defined. By exploiting the weakness of the policy, attackers can bypass the security rules that can lead to policy violations. For example, TCP packets with SYN and RST flags enabled or an IP packet length can exceed the actual length specified in the standards. Although this packet can bypass security rules, if the remote device is not able to handle this erroneous packet, it leads to a possible attack. Table. 1.2.2 below summarizes the technology weaknesses that include protocol weaknesses, operating system weaknesses, and network equipment weaknesses.

Weakness	Description
TCP/IP Applications and protocols	HTTP, FTP, SNMP, SMTP, TCP, IP, and DNS are implemented as per the standards and specifications which have inherent limitations that can be exploited
Operating system	Microsoft Windows, Apple Macintosh, IBM OS/2, UNIX, and other operating systems have several security issues
Network device	Password weaknesses like default passwords not changed or lack of strong passwords requirement, authentication weaknesses, firewall holes, and user interface weaknesses

Table 1.2.2 Technology weaknesses that affect networks

3. Configuration weaknesses

Network administrators need to have adequate skills to configure networks and network devices to prevent security threats. Table below describes some of the possible configuration weaknesses.

Weakness	Description
User Accounts	User accounts stored on devices must be secured. Exposing usernames and passwords can be a security threat.
Passwords	Password policy should be enforced at the user level. Passwords of major devices such as servers, routers, databases, should follow password policy set by the IT policy of the organization. Default passwords should not be allowed to be continued. The password secrecy should be preserved. These passwords have to be changed when an administrator leaves the organization. Passwords have to be periodically changed.
Configuration of TCP ports and Internet services	Should have a policy to define what application services should be allowed and for what purposes. A common problem is the lack of clarity in this regard and enabling some of the attack-prone ones like Java Script and VB Script or enabling the remote services or such other services without understanding the risks.
Default settings	If the network administrators do not change the default policy of the devices, it can cause serious security threats, such as default passwords are known to public, default permissions may be continued giving scope for attacks.
Mis-configuration of security and network devices	Mis-configuration of firewall and other network devices can cause serious security problems. For example, mis-configuration of access lists, routing protocol can cause serious security threats.

Table 1.2.3 Configuration weaknesses that affect networks

1.2.2 Threats

Internal threats and external threats are the two primary classes of threats to network security. They are illustrated in below Fig. 1.2.1. These threats are caused by attackers.

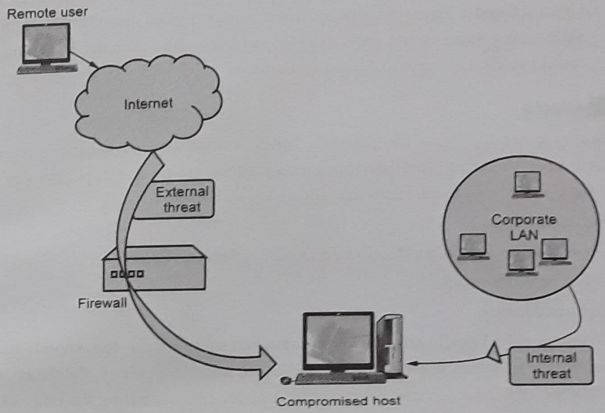

Fig. 1.2.1 Types of threats

Types of Threats

- **Internal threats :** Internal threats are threats from someone within the organization, who has proper access to the network and network resources, who understands the network infrastructure well, who understands the security applications and the security loop holes. Someone within the organization can create and send out attacks by hiding his identity as he already knows enough inside information. According to the FBI, 80 percent of the reported security incidents are due to internal access and misuse of information by an insider of the company.
- **External threats :** External threats are threats from outside the organization. They do not possess authorized access to the network resources. They work by gaining unauthorized access to the network and network resources with the intention of damaging the resources or for profit. These can be structured or unstructured :
  - **Structured :** Structured attacks come from technically competent hackers who belong to a class of highly motivated individuals. They understand vulnerabilities and develop sophisticated tools and techniques to penetrate without anyone knowing. These groups (also called hackers or crackers) may often be found to be involved in major crimes such as credit card theft or identity theft.

- **Unstructured** : These threats are from inexperienced individuals testing their skills using some of the tools available in the public domain. Sometimes, these can do serious damage to company assets.

1.2.2.3 Attacks

Attackers generally abuse the network "rules" established by security policies. The rules are broken in such a way that attackers send their traffic that appears to be normal traffic. Attacks can be classified into the following categories,

- Reconnaissance
- Denial of Service (DOS)/Distributed Denial of Service (DDoS)
- Other network attacks
- **Reconnaissance**

  To effectively launch an attack, the attacker should have the knowledge of the network, hardware used, software deployed, and its topology. Before an attack is launched, the attacker tries to gain this knowledge by scanning the network, which is called *reconnaissance*. Reconnaissance is not an attack by itself; however, this could cause a serious security threat by allowing the weaknesses of the network or network resources to be made known to the attacker. This is more an information-gathering mission.

  Quite often, reconnaissance is not detected for a considerable amount of time because they have no impact on the network.

  Sniffing is one of the important reconnaissance methods used by the attackers to collect the information, such as user IDs and passwords, other information like session id, transactions being carried out, other confidential details, and business discussions carried out. Other popular methods used are pinging, banner grabbing, and port scanning.

- **Denial-of-Service (DoS)and Distributed Denial-of-Service (DDoS)**

  The purpose of the DoS attack, as shown in below Fig. 1.2.2, is to make the network resources inaccessible to the user and bring down the network itself by generating a huge amount of network traffic that overwhelms or crashes the server, exceeding the capacity of the routers and switches, overwhelming the CPU and memory utilization.

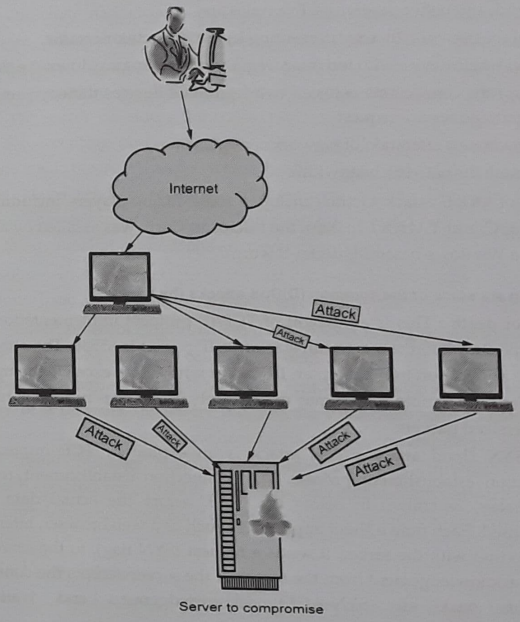

Fig. 1.2.2 Distributed denial of service attack

In some cases, DoS attacks can target a specific device and cause the system to hang.

Sometimes, the attacker gets into one device in the network remotely and triggers simultaneous exploitation of systems on the network or uses multiple compromised machines to initiate simultaneous attacks, causing interruptions of network and network resources. The sudden increase in the network traffic can cause the server or router to go down quickly and become inaccessible to the legitimate users. This kind of an attack is called a Distributed Denial-of-Service (DDOS) attack which hides the true origin of the attack.

- **Distributed Denial of Service Attack**

  A DoS (DDoS) attack is an explicit attack to prevent legitimate users from accessing network and network services. Examples are,

- Flood the network, thereby preventing legitimate network traffic.
- Target single device with too many requests thus bringing down the device.
- Disrupt the connections between two legitimate devices thereby preventing access to a genuine service request.
- Destruction or alteration of network configurations.
- Consume the network bandwidth.

The list of DDoS attack victims includes some major players including Microsoft, Amazon, HSBC, and YAHOO. In 2004, the Microsoft Corp. was assailed by a DDoS attack induced by a Windows-based Mydoom-B worm.

The following are some of the common (D)DoS attacks (by name),

- **Ping of death :** This is an exploit of TCP/IP protocol implementation. As per the RFC specification, the maximum size of an IP packet is 65536. The attacker uses the "ping" application to make up an IP packet whose size exceeds the maximum size specified. The remote system may crash or reboot if it does not know how to handle the oversized packets.
- **TCP SYN flood attack :** This attack is an exploit of TCP implementation of connection establishment process. TCP connection establishment requires three handshakes, as shown in below Fig. 1.2.3, before the actual data starts being transmitted. Each time a client application, such as a web browser, attempts to open a connection with the server, it sends a request (SYN flag), to the server and waits for the acknowledgement from the server. If the server accepts the connection, then it sends back an (SYN-ACK) acknowledgement and waits for the acknowledgement.

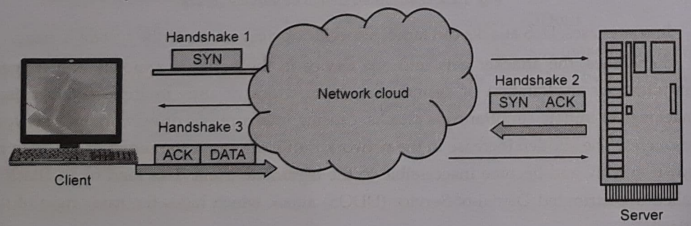

Fig. 1.2.3 TCP 3 way connection handshake

- Once the client receives the acknowledgement from the server, it sends one more segment (ACK) acknowledging the receipt of the server's information. Once both the server and client handshake completes, the actual data transmission starts. This is sometimes referred to as TCP 3-way handshake. Since each connection information takes up memory and CPU resources, only a limited number of in-progress connections are possible. When the server establishes connection with the client, the server considers the connection as open and frees up the queued resources for accepting new connections. During a SYN flood attack, the server never sends back the ACK packet to the hostile client. Instead, the hostile client application keeps sending repeated SYN requests causing DoS. The attacking application generates spoofed packets that appear to be valid new connections and enter into the queue, but connections are never completed .
- E-mail bombs - An Application program that can send bulk e-mails to individuals, organizations, lists, or domains to vandalize an e-mail server
- Teardrop - An IP protocol exploit where the IP packet is fragmented in such a way that reassembling the packet can cause the system to crash
- Smurf attack - Internet Control Message Protocol (ICMP) is used to test the availability of a network device by pinging the concerned node to determine its operational status. When the remote host sends a PING, the end device responds by sending a "reply" message. A smurf is a type of DoS attack in which a system is flooded with spoofed ping (ICMP) messages. This creates high network traffic and high consumption of network bandwidth and leads ultimately to the crashing of the remote system.
- **Other Attacks on Networks**

  Apart from the attacks that described above, there are other attacks that can cause serious damage to the network security. Some common ones include spoofing attacks, HTTP tunneling and session hijacking :

- **Masquerade/Spoofing attacks :** The network intruder masquerades the TCP/IP packet by an illegal IP address, falsifying the source address. The intruder fools the remote machine by an illegitimate source address but with valid user access privileges. In an IP spoofing attack, a malicious hacker from outside the network hacks into the network pretending to be an insider, a trusted user, of the organization and spoofs the source address of a legitimate inside user thus gaining access to the network resources. This attack can also cause a broadcast in the network causing high network traffic. If the attacker manages to alter the routing

tables, then response from the network resource can go to the spoofed destination address.

- **ARP spoofing and DNS spoofing :** The Address Resolution Protocol (ARP) spoofing is used to confuse the system to map incorrect MAC address to a particular IP address in the ARP table. Similarly DNS (Domain Name Service protocol) spoofing is to change the mapping of DNS entries in the DNS cache. Mac Flooding attacks are also similar to this.
- **HTTP tunneling :** This method may be used by the insiders to overcome the firewall controls and send confidential information to the outside world without anyone inside being aware of the same.
- **SSH tunneling :** These may be used to directly connect to a network stealthily and initiate attacks. This is an illegitimate use of a legitimate tool.
- **Session hijacking :** A session between the user and the server can be hijacked by the attacker. Some of the methods used in this regard are session fixing and session rediction. Here, usually a valid session between the user and server is taken over by the attacker.
- **Attacks on network equipment including routers :** The network equipment is traditionally prone to default password vulnerabilities because the network administrators not taking sufficient care in resetting these passwords. The weakness of the network configurations of a router is a new point of vulnerability. In addition to the administrator passwords, some vendors have a so-called "back-door" to their system for debugging purposes and to support the client in case an admin password is forgotten or lost. This back-door could also be exploited, if it is known to the attackers.

  - **Preventive Measures to Deal with Network Attacks**

1. Hardening of all network equipment with appropriate configurations and appropriate patching including firmware updates.
2. All default passwords to be substituted with strong passwords.
3. Defense in depth is implemented to avoid attacks like session hijacking.
4. Use safe session ID handling.
5. Session time-out to be set as appropriate to the application and its risks.
6. Set complicated session ID creation logic.
7. Use encrypted handshakes like SSL with Digital certificate or TLS, techniques like VPN.

8. Do not store passwords or critical information in the cookies.
9. Ensure that all the software used including utilities / tools are patched / updated.
10. Set easy-to-understand and clear security policies.
11. Create awareness among the employees on what can go wrong and what is expected from them - do's and don'ts.
12. Do not have the same user name and passwords for all the systems - use different ones
13. Logout promptly after the work is over.
14. Ensure cookies, history and offline content are removed after sensitive transaction sessions.
15. Do not click on the links in the suspect e-mails.

1.2.3 Security Policy - Concept and Related Information

In business, a security policy is a document that states in writing how a company plans to protect the company's physical and information technology (**IT**) assets. A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change. A company's security policy may include an **acceptable use policy,** a description of how the company plans to educate its employees about protecting the company's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

Simply, an information security policy is a statement or a collection of statements, designed to guide employees' behavior with regard to the security of company information and IT systems, etc. These security policies support the CIA triad and define the who, what and why regarding the desired behavior and they play an important role in an organization's overall security posture.

An **Information Technology** (IT) **Security Policy** identifies the rules and procedures for all individuals accessing and using an organization's IT assets and resources. Effective IT Security Policy is a model of the organization's culture, in which rules and procedures are driven from its employees' approach to their information and work. Thus, an effective IT security policy is a unique document for each organization, cultivated from its people's perspectives on risk tolerance, how they see and value their information and the resulting availability that they maintain of that information. For this reason, many companies will

find a boilerplate IT security policy inappropriate due to its lack of consideration for how the organization's people actually use and share information among themselves and to the public.

1.2.3.1 Importance of Information Security Policy

Creating an effective information security policy and ensuring compliance is a critical step in preventing security incidents like **data leaks** and **data breaches**.

ISPs are important for new and established organizations. Increasing digitalization means every employee is generating data and a portion of that data must be protected from unauthorized access. Depending on your industry, it may even be protected by laws and regulations.

Sensitive data, Personally Identifiable Information (PII), and intellectual property must be protected to a higher standard than other data.

Whether you like it or not, **information security** (InfoSec) is important at every level of your organization. And outside of your organization.

Increased outsourcing means third-party vendors have access to data too. This is why **third-party risk management** and **vendor risk management** is part of any good information security policy. **Third-party risk, fourth-party risk** and **vendor risk** are no joke.

1.2.3.2 Key Elements of an Information Security Policy

An information security policy can be as broad as you want it to be. It can cover IT security and/or physical security, as well as social media usage, lifecycle management and security training. In general, an information security policy will have these nine key elements :

1. Purpose and need of information security policy

Purpose of information security policy

- To create an organizational model for information security.
- To detect and preempt information security breaches caused by third-party vendors, misuse of networks, data, applications, computer systems and mobile devices.
- To protect the organization's reputation.
- To uphold ethical, legal and regulatory requirements.
- To protect customer data and respond to inquiries and complaints about non-compliance of security requirements and data protection.

Need of an Information Security Policy

The goal when writing an organizational information security policy is to provide relevant direction and value to the individuals within an organization with regard to security. While entire books have been published regarding how to write effective security policies, there are a few core reasons why any organization should have information security policies,

1. Information security policies define what is required of an organization's employees from a security perspective and establish a general approach to **information security**.
2. Information security policies reflect the **risk appetite** of an organization's management and should reflect the managerial mindset when it comes to security.
3. Information security policies provide direction upon which a **control framework** can be built to secure the organization against external and **internal threats**.
4. Information security policies are a mechanism to support an organization's legal and ethical responsibilities.
5. Information security policies are a mechanism to hold individuals accountable for compliance with expected behaviors with regard to information security.
6. Document security measures and **user access control** policies.
7. Detect and minimize the impact of compromised information assets such as misuse of data, networks, mobile devices, computers and applications.
8. Protect the reputation of the organization.
9. Comply with legal and regulatory requirements like NIST, GDPR, HIPAA and FERPA.
10. Protect their customer's data, such as credit card numbers.
11. Provide effective mechanisms to respond to complaints and queries related to real or perceived cyber security risks such as **phishing, malware** and **ransomware**.
12. Limit access to key information technology assets to those who have an acceptable use

2. Audience

Define who the information security policy applies to and who it does not apply to. You may be tempted to say that third-party vendors are not included as part of your information security policy.

This may not be a great idea. **Third-party, fourth-party risk** and **vendor risk** should be accounted for. Whether or not you have a legal or regulatory duty to protect your customer's data from third-party **data breaches** and **data leaks** isn't important. Customers may still blame your organization for breaches that were not in your total control and the reputational damage can be huge.

3. Information security objectives

These are the goals management has agreed upon, as well as the strategies used to achieve them.

The objectives of an IT security policy is the preservation of confidentiality, integrity and availability of systems and information used by an organization's members. These three principles compose the CIA triad :

- **Confidentiality** involves the protection of assets from unauthorized entities
- **Integrity** ensures the modification of assets is handled in a specified and authorized manner
- **Availability** is a state of the system in which authorized users have continuous access to said assets

The IT security policy is a living document that is continually updated to adapt with evolving business and IT requirements. Institutions such as the International Organization of Standardization (ISO) and the U.S. National Institute of Standards and Technology (NIST) have published standards and best practices for security policy formation. As stipulated by the National Research Council (NRC), the specifications of any company policy should address :

1. Objectives
2. Scope
3. Specific goals
4. Responsibilities for compliance and actions to be taken in the event of noncompliance.

Also mandatory for every IT security policy are sections dedicated to the adherence to regulations that govern the organization's industry. Common examples of this include the PCI Data Security Standard and the Basel Accords worldwide, or the Dodd-Frank Wall Street Reform, the Consumer Protection Act, the Health Insurance Portability and Accountability Act and the Financial Industry Regulatory Authority in the United States. Many of these regulatory entities require a written IT security policy themselves.

An organization's security policy will play a large role in its decisions and direction, but it should not alter its strategy or mission. Therefore, it is important to write a policy that is drawn from the organization's existing cultural and structural framework to support the continuity of good productivity and innovation, and not as a generic policy that impedes the organization and its people from meeting its mission and goals.

Without information security, an organization's information assets, including any intellectual property, are susceptible to compromise or theft. As a result, consumer and shareholder confidence and reputation suffer potentially to the point of ruining the company altogether. It is important to keep the principles of the CIA triad in mind when developing corporate information security policies.

4. Authority and access control policy

This part is about deciding who has the authority to decide what data can be shared and what can't. Remember, this may not be always up to your organization. For example, if you are the CSO at a hospital. You likely need to comply with HIPAA and its data protection requirements. If you store medical records, they can't be shared with an unauthorized party whether in person or online.

An **access control** policy can help outline the level of authority over data and IT systems for every level of your organization. It should outline how to handle **sensitive data,** who is responsible for security controls, what access control is in place and what security standards are acceptable.

It may also include a **network security** policy that outlines who can have access to company networks and servers, as well as what authentication requirements are needed including **strong password requirements, biometrics**, ID cards and access tokens.

In some cases, employees are contractually bound to comply with the information security policy before being granted access to any information systems and data centers.

5. Data classification

An information security policy must classify data into categories. A good way to classify the data is into five levels that dictate an increasing need for protection :

1. **Level 1 :** Public information
2. **Level 2 :** Information your organization has chosen to keep confidential but disclosure would not cause material harm.
3. **Level 3 :** Information has a risk of material harm to individuals or your organization if disclosed.

4. **Level 4 :** Information has a high risk of causing serious harm to individuals or your organization if disclosed.
5. **Level 5 :** Information will cause severe harm to individuals or your organization if disclosed.

In this classification, levels 2-5 would be classified as confidential information and would need some form of protection.

6. Data support and operations

Once data has been classified, there is a need to outline how data is each level will be handled. There are generally three components to this part of your information security policy :

1. **Data protection regulations :** Organizations that store **personally identifiable information (PII)** or **sensitive data** must be protected according to organizational standards, best practices, industry compliance standards and regulation.
2. **Data backup requirements :** Outlines how data is backed up, what level of **encryption** is used and what third-party service providers are used.
3. **Movement of data :** Outlines how data is communicated. Data that is deemed classified in the above data classification should be securely communicated with encryption and not transmitted across public networks to avoid **man-in-the-middle attacks**.

7. Security awareness training

A perfect information security policy that no one follows is no better than having no policy at all. You need your staff to understand what is required of them. Training should be conducted to inform employees of security requirements, including data protection, data classification, access control and general **cyber threats**.

Security training should include :

- **Social engineering :** Teach your employees about phishing, **spearphishing** and other common social engineering **cyber attacks**.
- **Clean desk policy :** Laptops should be taken home and documents shouldn't be left on desks at the end of the work day
- **Acceptable usage :** What can employees use their work devices and Internet for and what is restricted ?

8. Responsibilities and duties of employees

This is where you operationalize your information security policy. This part of your information security policy needs to outline the owners of :

- Security programs
- Acceptable use policies
- Network security
- Physical security
- Business continuity
- Access management
- Security awareness
- Risk assessments
- **Incident response**
- **Data security**
- Disaster recovery
- Incident management

9. Other items an ISP may include

Virus protection procedure, malware protection procedure, **network intrusion detection** procedure, remote work procedure, technical guidelines, consequences for non-compliance, physical security requirements, references to supporting documents, etc.

Best practices for information security management

A mature information security policy will outline or refer to the following policies,

1. **Acceptable Use Policy (AUP) :** Outlines the constraints an employee must agree to use a corporate computer and/or network.
2. **Access Control Policy (ACP) :** Outlines access controls to an organization's data and information systems.
3. **Change management policy :** Refers to the formal process for making changes to IT, software development and security.
4. **Information security policy :** High-level policy that covers a large number of security controls.
5. **Incident response (IR) policy :** An organized approach to how the organization will manage and remediate an incident.

6. **Remote access policy :** Outlines acceptable methods of remotely connecting to internal networks.
7. **Email/communication policy :** Outlines how employees can use the business's chosen electronic communication channel such as email, slack or social media.
8. **Disaster recovery policy :** Outlines the organization's cybersecurity and IT teams input into an overall business continuity plan.
9. **Business continuity plan (BCP) :** Coordinates efforts across the organization and is used in the event of a disaster to restore the business to a working order.
10. **Data classification policy :** Outlines how your organization classifies its data.
11. **IT operations and administration policy :** Outlines how all departments and IT work together to meet compliance and security requirements.
12. **SaaS and cloud policy :** Provides the organization with clear cloud and SaaS adoption guidelines, this helps mitigate **third-party** and **fourth-party risk**.
13. **Identity access and management (IAM) policy :** Outlines how IT administrators authorize systems and applications to the right employees and how employees create passwords to comply with security standards.
14. **Data security policy :** Outlines the technical requirements and acceptable minimum standards for data security to comply with relevant laws and regulations.
15. **Privacy regulations :** Outlines how the organization complies with government-enforce regulations such as GDPR that are designed to protect customer privacy.
16. **Personal and mobile devices policy :** Outlines if employees are allowed to use personal devices to access company infrastructure and how to reduce the risk of exposure from employee owned assets.

1.2.4 Picking Right Security Policy

There are two parts to any security policy. One deals with preventing external threats to maintain the integrity of the network. The second deals with reducing internal risks by defining appropriate use of network resources.

Addressing external threats is technology-oriented. While there are plenty of technologies available to reduce external network threats - firewalls, antivirus software, intrusion - detection systems, e-mail filters and others - these resources are mostly implemented by IT staff and are undetected by the user.

However, appropriate use of the network inside a company is a management issue. Implementing an acceptable use policy (AUP), which by definition regulates employee behavior, requires tact and diplomacy.

At the very least, having such a policy can protect organization from liability if one can show that any inappropriate activities were undertaken in violation of that policy. More likely, however, a logical and well-defined policy will reduce bandwidth consumption, maximize staff productivity and reduce the prospect of any legal issues in the future.

Since security policies should reflect the risk appetite of executive management in an organization, start with the defined risks in the organization. Write a policy that appropriately guides behavior to reduce the risk. If an organization has a risk regarding social engineering, then there should be a policy reflecting the behavior desired to reduce the risk of employees being socially engineered. One such policy would be that every employee must take yearly **security awareness training** (which includes social engineering tactics).

Since information security itself covers a wide range of topics, a company information security policy (or policies) are commonly written for a broad range of topics such as the following :

1. Access control
2. Identification and authentication (including **multi-factor authentication** and **passwords**)
3. Data classification
4. **Encryption**
5. **Remote access**
6. Acceptable use
7. **Patching**
8. **Malicious code protections**
9. Physical security
10. **Backups**
11. Server security (e.g. **hardening**)
12. Employee on/offboarding
13. **Change management**

The above list is just a sample of an organizational security policy (or policies). Compliance requirements also drive the need to develop security policies, but don't write a policy just for the sake of having a policy.

1.2.5 Strategies for Developing Suitable Information Security Policies for Organization

Following strategies provide common-sense approach to developing and implementing an appropriate security policy that will be fair, clear and enforceable.

1. Identify risks in organization

One of the primary purposes of a security policy is to provide protection - protection for your organization and for its employees. Security policies protect your organization's critical information/intellectual property by clearly outlining **employee responsibilities** with regard to what information needs to be safeguarded and why. When the what and why is clearly communicated to the who (employees) then people can act accordingly as well as be held accountable for their actions. Employees are protected and should not fear reprisal as long as they are acting in accordance with defined security policies.

Another critical purpose of security policies is to support the mission of the organization. Security professionals need to be sensitive to the needs of the business, so when writing security policies, the mission of the organization should be at the forefront of your thoughts. Ask yourself, how does this policy support the mission of my organization ? Is it addressing the concerns of senior leadership? What are your risks from inappropriate use ? Do you have information that should be restricted ? Do you send or receive a lot of large attachments and files ? Are potentially offensive attachments making the rounds ? It might be a nonissue. Or it could be costing thousands of rupees per month in lost employee productivity or computer downtime.

Of course, in order to answer these questions, you have to engage the senior leadership of your organization. What is their sensitivity toward security ? If they are more sensitive in their approach to security, then the policies likely will reflect a more detailed definition of employee expectations. This approach will likely also require more resources to maintain and monitor the enforcement of the policies. A less sensitive approach to security will have less definition of employee expectations, require fewer resources to maintain and **monitor policy** enforcement, but will result in a greater risk to your organization's intellectual assets/**critical data**.

Either way, do not write security policies in a vacuum. If you do, it will likely not align with the needs of your organization. Writing security policies is an iterative process and will require buy-in from executive management before it can be published.

A good way to identify your risks can be through the use of monitoring or reporting tools. Many vendors of firewalls and Internet security products allow evaluation periods for their products. If those products provide reporting information, it can be helpful to

use these evaluation periods to assess your risks. However, it's important to ensure that your employees are aware that you will be recording their activity for the purposes of risk assessment, if this is something you choose to try. Many employees may view this as an invasion of their privacy if it's attempted without their knowledge.

2. Make your security policies brief and succinct

Security policies should not include everything but the kitchen sink. Supporting procedures, baselines, and guidelines can fill in the "how" and "when" of your policies. Each policy should address a specific topic (e.g. acceptable use, access control, etc.); it will make things easier to manage and maintain.

Keep it simple don't overburden your policies with technical jargon or legal terms. Use simple language; after all, you want your employees to understand the policy. When employees understand security policies, it will be easier for them to comply. When writing security policies, keep in mind that "complexity is the worst enemy of security" (Bruce Schneier), so keep it brief, clear, and to the point.

3. Make sure the policy conforms to legal requirements

Depending on your data holdings, jurisdiction and location, you may be required to conform to certain minimum standards to ensure the privacy and integrity of your data, especially if your company holds personal information. Having a viable security policy documented and in place is one way of mitigating any liabilities you might incur in the event of a security breach.

4. Level of security = level of risk

Don't be overzealous. Too much security can be as bad as too little. You might find that, apart from keeping the bad guys out, you don't have any problems with appropriate use because you have a mature, dedicated staff. In such cases, a written code of conduct is the most important thing. Excessive security can be a hindrance to smooth business operations, so make sure you don't overprotect yourself.

5. Ensure your security policies are enforceable

If the policy is not going to be enforced, then why waste the time and resources writing it? It is important that everyone from the CEO down to the newest of employees comply with the policies. If upper management doesn't comply with the security policies and the consequences of non-compliance with the policy is not enforced, then mistrust and apathy toward compliance with the policy can plague your organization.

Look across your organization. Can the policy be applied fairly to everyone? If not, rethink your policy. Security policies are supposed to be directive in nature and are intended to guide and govern employee behavior. If the policy is not enforced, then employee behavior is not directed into productive and secure computing practices which results in greater risk to your organization. Users need to be exposed to security policies several times before the message sinks in and they understand the "why" of the policy, so think about graduating the consequences of policy violation where appropriate.

Another important element of making security policies enforceable is to ensure that everyone reads and acknowledges the security policies (often via signing a statement thereto). Many security policies state that non-compliance with the policy can lead to administrative actions up to and including termination of employment, but if the employee does not acknowledge this statement, then the enforceability of the policy is weakened.

6. Include staff in policy development

No one wants a policy dictated from above. Involve staff in the process of defining appropriate use. Keep staff informed as the rules are developed and tools are implemented. If people understand the need for a responsible security policy, they will be much more inclined to comply.

7. Train your employees

Staff training is commonly overlooked or underappreciated as part of the AUP implementation process. But, in practice, it's probably one of the most useful phases. It not only helps you to inform employees and help them understand the policies, but it also allows you to discuss the practical, real-world implications of the policy. End users will often ask questions or offer examples in a training forum, and this can be very rewarding. These questions can help you define the policy in more detail and adjust it to be more useful.

8. Get it in writing

Make sure every member of your staff has read, signed and understood the policy. All new hires should sign the policy when they are brought on board and should be required to reread and reconfirm their understanding of the policy at least annually. For large organizations, use automated tools to help electronically deliver and track signatures of the documents. Some tools even provide quizzing mechanisms to test user's knowledge of the policy.

9. Set clear penalties and enforce them

Network security is no joke. Your security policy isn't a set of voluntary guidelines but a condition of employment. Have a clear set of procedures in place that spell out the penalties for breaches in the security policy. Then enforce them. A security policy with haphazard compliance is almost as bad as no policy at all.

10. Explain how policy exceptions are handled

You've heard the expression, "there is an exception to every rule." Well, the same perspective often goes for security policies. There are often legitimate reasons why an exception to a policy is needed. In these cases, the policy should define how approval for the exception to the policy is obtained. Management should be aware of exceptions to security policies as the exception to the policy could introduce risk that needs to be mitigated in another way.

11. Update your staff

A security policy is a dynamic document because the network itself is always evolving. People come and go. Databases are created and destroyed. New security threats pop up. Keeping the security policy updated is hard enough, but keeping staffers aware of any changes that might affect their day-to-day operations is even more difficult. Open communication is the key to success.

12. Install the tools you need

Having a policy is one thing, enforcing it is another. Internet and e-mail content security products with customizable rule sets can ensure that your policy, no matter how complex, is adhered to. The investment in tools to enforce your security policy is probably one of the most cost-effective purchases you will ever make.

13. Learn from others

There are many types of security policies, so it's important to see what other organizations like yours are doing. You can spend a couple of hours browsing online, or you can buy a book such as ***Information Security Policies Made Easy*** by Charles Cresson Wood, which has more than 1,200 policies ready to customize. Also, talk to the sales reps from various security software vendors. They are always happy to give out information.

1.2.6 Keeping Security Policies Updated and Living with Continuously Changing IT World

The purpose of security policies is not to adorn the empty spaces of your bookshelf. Security policies can stale over time if they are not actively maintained. At a minimum,

security policies should be reviewed yearly and updated as needed. It is good practice to have employees acknowledge receipt of and agree to abide by them on a yearly basis as well.

In preparation for this event, review the policies through the lens of changes your organization has undergone over the past year. What new threat vectors have come into the picture over the past year ? What have you learned from the security incidents you experienced over the past year ? Take these lessons learned and incorporate them into your policy. Security policies are living documents and need to be relevant to your organization at all times.

Types if security policy (Important Cyber Security Policies Recommendations)

1. Virus and spyware protection policy

The Virus and Spyware Protection policy provides the following protection,

- It helps to detect, removes, and repairs the side effects of viruses and security risks by using signatures.
- It helps to detect the threats in the files which the users try to download by using reputation data from download insight.
- It helps to detect the applications that exhibit suspicious behaviour by using SONAR heuristics and reputation data. Download insight and SONAR technology are available only on windows clients.

2. Firewall policy

Firewall policy provides the following protection,

- It blocks the unauthorized users from accessing the systems and networks that connect to the internet.
- It detects the attacks by cybercriminals.
- It removes the unwanted sources of network traffic. Firewall policies can be applied only to windows clients.

3. Intrusion prevention policy

This policy automatically detects and blocks the network attacks and browser attacks. It also protects applications from vulnerabilities. It checks the contents of one or more data packages and detects malware that can arrive through legal path.

4. Live update policy

This policy can be classified into two types one is LiveUpdate Content policy and another is live update setting policy. The live update policy contains the setting which determines when and how client computers download the content updates from live update. One can define the computer that clients contact to check for updates and schedule when and how often clients computer check for updates that are required.

5. Application and device control

The application and device control policy protects a system's resources from applications and manages the peripheral devices that can attach to computers. Application control policy can be applied only to windows clients. The device control policy applies to windows and mac computers.

6. Host integrity policy

This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure. One can use this policy to ensure that the client's computers who access our network are protected and compliant with company's securities policies. This policy requires that the client system must have installed antivirus.

7. Memory exploit mitigation

The Memory Exploit Mitigation policy stops vulnerability attacks on software using mitigation techniques such as DLL hijacking, heap spray mitigation, and Java exploit prevention. This policy type was added for 14.0.1. Version 14 added this functionality in the Intrusion Prevention policy under the name of Generic Exploit Mitigation.

8. Exceptions policy

This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans and by SONAR. One can also exclude applications from application control.

9. Web and cloud access protection

Web and cloud access protection sends network traffic to a Symantec Web Security Service (WSS). The WSS solution protects users and organizations by categorizing applications and web sites, and then allowing or denying access to them based on policy. Web and Cloud Access Protection was renamed from Network Traffic Redirection in 14.3 RU2.

1.3 Host Based Security

1.3.1 Host

Host is a source of information or signals. The term can refer to a computer, smart phone, tablet or any electronic device. In a network, clients (users' machines) and servers are hosts because they are both sources of information in contrast to network devices, such as routers and switches, which only direct traffic.

A Host-Based System

It is a system controlled by a central or main computer. A host-based system may refer to a hierarchical communications system controlled by a central computer.

Host-Based Security

Along with server and **network security,** host security should be among a network's top security priorities. Furthermore, the most dangerous element in an organization is the end-users as they will directly interact with the company's resources and network. This is why cybersecurity professionals need to secure their networks and resources against the potential threats from end-users, removable media, and peripherals.

With the advancement in technology, number of devices connecting to the network are also increasing and organization need to implement security policies, especially when these are not corporate devices. From handheld devices like phones and tablets, to the new work-from-home environment, there are more and more types of devices (hosts) being added to a network. It is of utmost importance that these devices are protected at all times, both software and hardware included. This is where host security comes in.

Security in host-based computing continues to be a critical issue in network security. Problems in host-based security exist in three principal areas,

i) Application protection
ii) Host environment protection
iii) Data protection.

1.3.2 Managing Devices and Host Security

Two general areas that must be covered when dealing with network security devices are :

- Using protocols and software for protecting data. This method involves using software to help an organization protect internal network components like personal host-based firewalls and antivirus software.

- Addressing the physical components like network components, hardware and physical security designs for securing the device.

1.3.3 Ensuring Server Security

Host security is an important part of server management for server administrators and web hosting providers. Some of the network security techniques that one can use are stated below.

1. Public key authentication for SSH

Organizations that want to secure their network needs to avoid using unencrypted access and opt for **SSH,** https, and SFTP. For better security, the organization should use SSH keys instead of password authentication on SSH. With this **network security** method, there will be no risk of a successful brute force attack on a weak password.

2. Strong passwords

A secured server is usually a challenge for criminals. However, many server administrators often leave their server unsecured by using easily guessed passwords. Therefore it is best to use **long** and **random passwords** for restricting users with login type access.

3. Firewalls

A host-based **firewall** is a software or hardware device that helps to control how a service is exposed to a network and the types of traffic that can enter or go out of a given server. For better host security, organizations need a properly configured firewall to ensure that only publicly available services can be reached outside your servers.

4. Malware scanning software

You need a network defense mechanism to keep malicious individuals out of your server. Although some malicious individuals will manage to breach your server's security, you will want to know about this as soon as possible. You will find lots of malware scanning software that you can install on your server.

5. Keep software up-to-date

Generally, out-of-date software may likely comprise of security weaknesses that hackers can use to breach your server. Therefore organizations need to ensure that they use updated software.

6. Regular backup

Although this may not be considered as a security measure, the major reason for securing a server is to keep the data stored. Since it is impossible to guarantee that a server will not be breached, organizations need to back up and encrypt their data in an offsite location. Organizations can then perform testing of recovery from backups regularly to neutralize ransomware attacks.

7. Monitor logs

One of the essential security tools is the log. This is because a server gathers information about what it does and who connects to it. Furthermore, the patterns in the data collected can then show the malicious behavior or security compromises. There are several apps that you can use to monitor your server's logs.

8. Other commonly used security techniques

Some of the other tips that one can use to manage your server and **network security** are turning off unnecessary services, isolate the execution environment, through file auditing and intrusion detection system, etc.

1.4 Perimeter Security

1.4.1 Network Perimeter

A network perimeter is the secured boundary between the private and locally managed side of a network, often a company's intranet, and the public facing side of a network, often the internet.

1.4.2 Types of Network Segments

Network segments can be classified into the following categories :

- **Public networks** allow accessibility to everyone. The internet is a perfect example of a public network. There is a huge amount of trivial and unsecured data on public networks. Security controls on these networks are weak.
- **Semi-private networks** sit between public networks and private networks. From a security standpoint, a semi-private network may carry confidential information but under some regulations.
- **Private networks** are organizational networks that handle confidential and propriety data. Each organization can own one or more private networks. If the organization is spread over vast geographical distances, the private networks at each location may be interconnected through the internet or other public networks.

- **Demilitarized zone (DMZ)** is a noncritical yet secure region at the periphery of a private network, separated from the public network by a firewall; it might also be separated from the private network by a second firewall. Organizations often use a DMZ as an area where they can place a public server for access by people they might not trust. By isolating a server in a DMZ, you can hide or remove access to other areas of your network. You can still access the server using your network, but others aren't able to access further network resources.
- **Software-defined networking (SDN)** is a relatively recent trend that can be useful both in placing security devices and in segmenting the network. Essentially, in an SDN, the entire network is virtualized, which enables relatively easy segmentation of the network. It also allows administrators to place virtualized security devices wherever they want.

1.4.3 Elements Making Up A Network Perimeter

- **Border routers :** Routers are the traffic cops of networks. Routers serve as the traffic signs of networks. They direct traffic into, out of, and throughout networks. The border router is the final router under the control of an organization before traffic appears on an untrusted network, such as the Internet.
- **Firewalls :** A firewall is a device that has a set of rules specifying what traffic it will allow or deny to pass through it. A firewall typically picks up where the border router leaves off and makes a much more thorough pass at filtering traffic. A firewall is a chokepoint device that has a set of rules specifying what traffic it will allow or deny to pass through it. A firewall typically picks up where the border router leaves off and makes a much more thorough pass at filtering traffic. Firewalls come in several different types, including static packet filters, stateful firewalls, and proxies. One might use a static packet filter such as a Cisco router to block easily identifiable "noise" on the Internet, a stateful firewall such as a Check Point FireWall-1 to control allowed services, or a proxy firewall such as Secure Computing's Sidewinder to control content.
- **Intrusion Detection System (IDS) :** This functions as an alarm system for your network that is used to detect and alert on suspicious activity. This system can be built from a single device or a collection of sensors placed at strategic points in a network. An IDS is like a burglar alarm system for your network that is used to detect and alert on malicious events. The system might comprise many different IDS sensors placed at strategic points in your network. Two basic types of IDS exist: network-based (NIDS), such as Snort or Cisco Secure IDS, and host-based (HIDS),

such as Tripwire or ISS BlackICE. NIDS sensors monitor network traffic for suspicious activity. NIDS sensors often reside on subnets that are directly connected to the firewall, as well as at critical points on the internal network. HIDS sensors reside on and monitor individual hosts.

- **Intrusion Prevention System (IPS) :** Compared to a traditional IDS which simply notifies administrators of possible threats, an IPS can attempt to automatically defend the target without the administrator's direct intervention. An IPS is a system that automatically detects and thwarts computer attacks against protected resources. Such protection may involve using signature-based or behavioral techniques to identify an attack and then blocking the malicious traffic or system call before it causes harm. In this respect, an IPS combines the functionality of a firewall and IDS to offer a solution that automatically blocks offending actions as soon as it detects an attack.
- **De - militarized zones / screened subnets :** DMZ and screened subnet refer to small networks containing public services connected directly to and offered protection by the firewall or other filtering device. The term DMZ originated during the Korean War when a strip of land at the 38th parallel was off-limits militarily. A DMZ is an insecure area between secure areas. Just as the DMZ in Korea was in front of any defenses, the DMZ, when applied to networks, is located outside the firewall. A firewall or a comparable traffic - screening device protects a screened subnet that is directly connected to it. It should be noted that a DMZ is in front of a firewall, whereas a screened subnet is behind a firewall. A screened subnet is an isolated network that is connected to a dedicated interface of a firewall or another filtering device. The screened subnet is frequently used to segregate servers that need to be accessible from the Internet from systems that are used solely by the organization's internal users. The screened subnet typically hosts "public" services, including DNS, mail and web. We would like to think these servers are bastion hosts. A bastion is a well - fortified position. When applied to hosts on a network, fortifying involves hardening the operating system and applications according to best practices. As attacks over time have shown, these servers are not always well fortified; in fact, they are sometimes vulnerable despite being protected by a firewall. We must take extra care fortifying these hosts because they are the target of the majority of attacks and can bring the attacker closer to accessing even more critical internal resources.

- **Virtual private networks :** It is a protected network session formed across an unprotected channel such as the Internet. Usually, a VPN is referred in terms of the device on the perimeter that enables the encrypted session, such as Cisco VPN Concentrator. The intended use might be for business partners, road warriors, or telecommuters. A VPN allows an outside user to participate on the internal network as if connected directly to it. Many organizations have a false sense of security regarding their remote access just because they have a VPN. However, if an attacker compromises the machine of a legitimate user, a VPN can give that attacker an encrypted channel into your network.
- **Software architecture :** Software architecture are the applications that are hosted on the organization's network, and it defines how they are structured. For example, we might structure an e-commerce application by splitting it into three distinct tiers,
  - The web front end that is responsible for how the application is presented to the user
  - The application code that implements the business logic of the application
  - The back-end databases that store underlying data for the application

Software architecture plays a significant role in the discussion of a security infrastructure because the primary purpose of the network's perimeter is to protect the application's data and services. When securing the application, one should ensure that the architecture of the software and the network is harmonious.

1.4.4 Network Perimeter Security

Perimeter security is the philosophy of setting up functional apparatus or techniques at the perimeter of the network to secure data and resources. It is part of the greater security field and has its own role in active system protection.

Perimeter security is comprised of systems like firewalls and browser isolation systems. Best practices in perimeter security include threat recognition, surveillance detection and pattern analysis.

Essentially, in perimeter security, security professionals are trying to create a perimeter-based approach to secure systems and ward off threats as they enter a network. However, many areas of today's security industry believe perimeter security to be less than entirely effective on its own. Other kinds of internal security are emerging to apply to high-quality security processes.

1.4.5 Network Perimeter Requirements

For most modern businesses, there is no single defensible boundary between a company's internal assets and the outside world.

- Internal users are not simply connecting from inside an organization's building, network, or inner circle. They are connecting from external networks and using mobile devices to access internal resources.
- Data and applications are no longer housed on servers that businesses physically own, maintain, and protect. Data warehouses, cloud computing, and software as a service present immediate access and security challenges for both internal and external users.
- Web services have opened a wide door to interactions outside of normal trust boundaries. To serve multiple clients, or simply to communicate with other services, both internal and external, insecure interactions on external platforms occur all the time.

Also, individually protecting each software application, service, or asset can be quite challenging. While the concept of a "network perimeter" has meaning for certain network configurations, in today's environment it should be treated abstractly, rather than as a specific setup.

1.4.6 Network Perimeter Guidelines

With this in mind, there are a few guidelines that can help to deliver a secure and modular network environment:

- Strong authentication to allow controlled access to information assets. Two factor authentication acts as an extra layer of security for logins, ensuring that attempted intrusions are halted before any damage is done.
- Hardening of mobile and IoT devices that connect to the network. Access control policies define high-level requirements that determine who may access information, and under what circumstances that information can be accessed.
- Embedded security services inside devices and applications. Embedded security solutions can help protect devices ranging from atm's to automated manufacturing systems. Features including application white listing, antivirus protection, and encryption can be embedded to help protect otherwise exposed IoT devices.
- Collecting security intelligence directly from applications and their hosts. Maintaining an open communication line with cloud service providers like AWS can greatly increase security protections. Application and service managers understand how to integrate shared security with their systems better than anyone else.

1.4.7 Network Perimeter Importance

The increasing reliance on an interconnected ecosystem of online devices in today's business environment has greatly increased our reliance on network security in order to prevent cyber attacks. Data is collected, collated, and interpreted on a massive scale, and it's security is dependent on the protections that surrounds it. The concept and evolution of a network perimeter allows organizations to think effectively on how to safeguard their internal information from untrusted or malicious actors.

1.5 Strategies for Secure Network

Generally, organizations should seek opportunities for the greatest overall increase in network security with the least amount of effort or expense. Encrypting network traffic is a first line of defense for protecting sensitive or confidential information sent over third-party networks, thus reducing some of the most significant security or privacy-related vulnerabilities due to negligent employees, unstable operating systems and other potential causes of a data loss or theft.

In the private sector, the network is the channel for conducting business in today's global marketplace. Protecting the network from threats and vulnerabilities can be daunting; however, there are strategies that can help organizations to protect the critical information assets traveling through their networks. These strategies are as follows,

1. Know your network infrastructure

Having visibility into your network infrastructure is crucial before you can even begin to secure your network against potential threats. Unless you know which hardware/software devices components comprise your network, you won't be able to protect them.

When formulating your network security strategy, you should take into account all your :

- Hardware (routers, switches, printers, etc.)
- Software (firewalls, IDS/IPS, etc.) devices, and
- Digital security certificates (SSL/TLS certificates, IoT certificates, etc.).

2. Take an umbrella approach covering every aspect

A business needs to protect both the data and the network because they work hand-in-glove. The data itself can be considered the currency of the digital world, so its protection is critical; the network moves the data, so it must be secured as well. Below activity are necessary to have a secure network,

1. **Conduct regular risk assessments :** Understand what types of data are traveling through the network. Take appropriate steps to protect confidential data, but be aware that clever insiders or thieves can access the network, take pieces of data, combine them and, as a result, put your organization's sensitive data at risk.

   Risk assessments need to take into consideration an organization's business model. First, analyze what types of data are most confidential if you are a retailer, bank, health-care provider or hospitality business. After classifying the sensitivity of an organization's data, security managers need to consider who needs access to data and how the data should be secured as it travels from point to point on the network. Risk assessments are critical to understanding how resources should be allocated to protect the network.

2. **Control and monitor the data traveling the network :** According to research conducted by the Ponemon Institute and CipherOptics, many IT professionals do not know whether their organizations permit clear text traffic when transmitting from host to host; or, whether they have controls in place to inform them about third-party data transfers.

3. **Support accountability at the leadership level :** How well does the organization's leadership understand and support the importance of protecting the network? Is there someone accountable? Without leadership's commitment to security, it is difficult, if not impossible, to achieve the recommendations listed here.

4. **Assemble a network security risk council :** The council should be composed of representatives from the following areas of an organization: security, legal, human resources, privacy, information technology, internal auditing and operations. The purpose is to determine what would be the greatest threat to the business if the network went down. This risk cannot be decided by the IT department alone. Risks are dependent upon the environment in which the business operates.

5. **Ensure enforcement of network security policies :** It is important to verify that policies are being followed and employees are in compliance. Employees can deliberately circumvent policies. Therefore, it is important to make sure that mechanisms are in place to detect noncompliance and punish negligent or malicious employees.

6. **Invest in robust and up-to-date network security technologies :** Make sure the network is patched to the proper levels, and that the hardware is current and maintained by the vendor. Blend encryption with smart cards, biometrics and analytic profiling. Encrypt everything, even at the chip level. Use network partitions

to select the "tunnels" the organization wants to protect. Scan the network to know where every device is. An alert system should be built into the network to shut down devices.

7. **Have an incident response plan in place :** Bad things can happen to good networks. While technology can help to protect the network, it is important to have plans in place to deal with network disruptions.

2. Implement Network Segmentation and Segregation Strategies

Handling security for a sizeable unsegmented network (with tasks such as defining firewall policies and effectively managing how the traffic flows) can be a complicated business. **Segmenting your network** into smaller chunks and establishing different trust zones can not only makes management easier but can also keep networks isolated in the event of a security incident, reducing the risks and impact of a network intrusion.

An unsegmented network provides potential hackers with a larger attack surface where they can move laterally through the network to access business-critical data. Such a breach can evade detection owing to the enormity of the network. Implementing network segmentation and segregation proves useful in such scenarios, giving you the control over how traffic moves within your environment.

3. Opt for a data loss prevention solution

Data exfiltration, or the unauthorized movement of data from an endpoint (either due to malware or insider threats), is a common occurrence within an organization. If your organization stores, processes, or transmits sensitive data (such as personally identifiable information [PII], payment card industry [PCI] data, client data, etc.), it may be subject to compliance regulation that makes it mandatory to protect such data. Irrespective of regulatory requirements, it makes sense to identify and keep track of events surrounding critical data to avoid any breaches.

4. Conduct awareness training for users and staff

Insider threats often emerge in the form of negligent employees who're unaware of network security best practices when it comes to maintaining good **cybersecurity hygiene.** While employees can be the easiest targets for attackers via **social engineering techniques** and **phishing emails,** they can also prove to be your best defense against potential security breaches.

Infosecinstitute.com reports that in a study of an unnamed Fortune 50 organization, where 35 % of the employees received training to identify fraudulent emails based on a

simulated phishing attack, the training led to an 84 % decrease in the chances of falling victim to such attacks.

Offering mandatory organization-wide cyber awareness programs, particularly when done on a regular basis, drives home the importance of network security basics, IT compliance, password security, etc. It also ensures that employees stay informed about different forms of cybersecurity threats.

5. Conduct third party vendor assessment

Working with third-party contractors may be unavoidable in some cases. However, if they're given access to your business network, it has an impact on the overall security of your organization. Because it increases the number of access points to your network, ensure that the security posture of these third-party vendors is carefully evaluated based on the level of access they require.

For instance, **Airbus** was attacked at least four times last year via its third - party supplier networks - Rolls Royce, Expleo and two others, according to bitsite.com. Hackers targeted virtual private networks to gain remote access to their business network in search of intellectual property of the aerospace manufacturer. Similarly, in the past, Target and several other organizations have fallen victim to attacks via external vendors.

6. Establish an incident management plan

An **incident management plan** provides guidance for how you can get your business from managing a cyber incident to when you return to normal operations. It provides structure and the necessary information your incident management and incident response teams need to do their jobs.

When an incident response plan is put into action, the incident response (IR) team comes into the picture in the event of a security breach that's detected by means of network security monitoring. They're responsible for escalating the incident to the appropriate teams and work on a timely resolution. Once the situation resolves, the next step is to recover systems to restore their proper functioning. A business continuity/disaster recovery plan can go a long way to ensure the availability of your network and associated systems.

The National Institute of Standards and Technology's (NIST) **Computer Security Incident Handling Guide** (800-61) also provides some great information regarding computer security incident response.

7. Administer regular software updates and patch management

Did you know that 27 % of reported breaches were the result of unpatched vulnerabilities ? **Data from Tripwire,** a security company, also indicates that unpatched vulnerabilities were also responsible for 34 % of data breaches for European organizations.

Updating and patching up software is crucial to preventing exploitation via any known vulnerabilities in applications developed in-house or through proprietary software. Be sure to install available security patches and updates for all your software within a targeted timeframe that's in line with the entire organization's risk management process.

8. Validate the security of network devices

All efforts to secure your network will be in vain if there are glaring security loopholes or bugs in your connected network devices. Ask yourself : How secure are the devices that have access to your network ? There are a few key things to consider :

- All network devices (servers, desktops, routers, etc.) should only be purchased from authorized resellers and well-reputed vendors.
- Also be sure to configure devices securely to turn off unnecessary services, disable unassigned or unused ports, manage default settings, etc.
- When updating your network equipment devices, make sure that patches are downloaded only from validated sources.

9. Protect your network against malware

Phishing scams are on the rise, and one can never be too careful when it comes to malware protection. Installing an endpoint protection solution (which typically includes anti-malware) on all your network's endpoints establishes a consistent, standardized, and distributed layer of security along your network perimeter.

Another way to protect your network from malware is to use email signing certificates/personal authentication certificates (PACs) for your email clients. If all of your employees are using these digital certificates, which attach digital signatures to every email, it helps to ensure that your employees can verify whether someone in your business really sent any questionable or suspicious emails.

10. Formulate an IT policy and enforce it

Clearly defined IT policies not only act as directives that empower your employees as they carry out their duties, but they also hold them accountable in case of non-

compliance. A network security policy governs how to implement and maintain security across the computer network. It outlines rules for access, operation, etc. under ordinary conditions and offers guidance on how to proceed in the event of a breach.

To enforce such policies, however, you need to ensure that your employees are aware of them. Data from **a Kaspersky Labs study** indicates that only 12 % of surveyed employees claim to know their organizations' IT security policies and requirements. These rules and policies should be part of not only the onboarding process, but they also should be included in regular cyber awareness trainings to keep them top of mind.

11. Deploy the right technology

There are several network security solutions that you'd want to take into consideration in terms of tools that need to be deployed to secure your environment. Some of these include :

- Intrusion detection systems/intrusion prevention systems (IDS/IPS),
- Firewalls,
- Virtual private networks (VPNs),
- Unified threat management (UTM) tools, and
- User and entity behavior analytics (UEBA) solutions.

Choose your technology in a way that they interoperate cohesively, especially in cases where the technology comes from various vendors.

12. Assemble the right security team and keep their skills current

According to **Cybersecurity Ventures,** by 2021, there will be 3.5 million unfilled jobs in the security industry with an ever-increasing skill gap. As several organizations compete to hire security professionals from a limited resource pool, assembling the right IT security team with the required skill set can be challenging.

However, it's of the utmost importance to build the right team to implement and manage your network (deploy tools, network threat monitoring, incident handling, etc.). It's just as important to provide them with the necessary training to upgrade and cultivate their skills continually.

13. Update passwords at least every quarter

Hopefully, by now your employees know to avoid default **passwords** or phrases like "password," "12345" and their dates of birth. In addition to using passwords that feature both letters, symbols and numbers and some uppercase letters for added security, require employees to regularly change any personal passwords used on systems that have access

to business networks (your business will have its own, but many computers also allow personal passwords).

Let employees know that when choosing passwords, substituting letters with similarly shaped characters, like "pa$$w0rd" for "password," is a bad idea. Hackers are onto that trick!

Every quarter is the recommended frequency, but more often is better. However, there is a fine line: changing passwords too often can cause confusion, leading employees to reach out to IT for reminders of their username and passwords (and we all know how much IT likes getting calls like that!).

14. Create a Virtual Private Network (VPN)

With millions of workers now working remotely because of the pandemic, there's been a 300 % increase in reported cybercrimes since COVID-19 began. VPNs create a far more secure connection between remote computers (home networks or computers used by people on the road) and other "local" computers and servers.

These networks are essentially only available to people who should have access to your systems, including your wireless network, and to equipment that's been authorized in your network settings. A VPN can dramatically decrease the likelihood of hackers finding a wireless access point and wreaking havoc on your system.

15. Filter and delete spam emails

Phishing emails from hackers are crafted in a way to entice your employees to open them and click on sensational offers or links. Spam filters have advanced considerably and should be leveraged. Even so, the occasional spam email may make it through, especially if a hacker is mimicking someone you know, like a professional colleague or company you do business with. Employees need to use their common sense filters in addition to any spam filter software.

16. Shut down computers when not in use

When is the last time you shut down your computer after a long day at work? When your computer is sitting idle overnight while connected to your company's network, it becomes more visible and available to hackers. By shutting down your computer, you're limiting their access to your network. And if they've already gained access, you're disrupting their connection.