UNIT-I

The Importance of Network Security

Network security is vital to maintaining the integrity of your data and the privacy of your organization and employees. It encompasses everything from the most basic practices, such creating strong passwords and fully logging out of community computers, to the most complex, high-level processes that keep networks, devices and their users safe. More and more sensitive information is stored online and in these various devices, and if an unauthorized user gains access to that data, it could lead to disastrous results.

Network security is the key to keeping that sensitive information safe, and as more private data is stored and shared on vulnerable devices, network security will only grow in importance and necessity. Experts expect that more than 2,314 exabytes (or over 2 trillion gigabytes) of data will exist by 2020; managing that amount of data is difficult enough, and protecting it will be another issue entirely.

While each and every member of your organization can take strides to help keep things secure, network security has become more complex in recent years. Adequately protecting networks and their connected devices requires comprehensive network training, a thorough understanding of how networks actually work and the skills to put that knowledge into practice. It's crucial for networks to be thoroughly and properly set up, secured and monitored to fully preserve privacy.

Common Network Security Vulnerabilities

In order to effectively implement and maintain secure networks, it's important to understand the common vulnerabilities, threats and issues facing IT professionals today. While some can be fixed fairly easily, others require more involved solutions.

Virtually all computer networks have vulnerabilities that leave them open to outside attacks; further, devices and networks are still vulnerable even if no one is actively threatening or targeting them. A vulnerability is a condition of the network or its hardware, not the result of external action.

These are some of the most common network vulnerabilities:

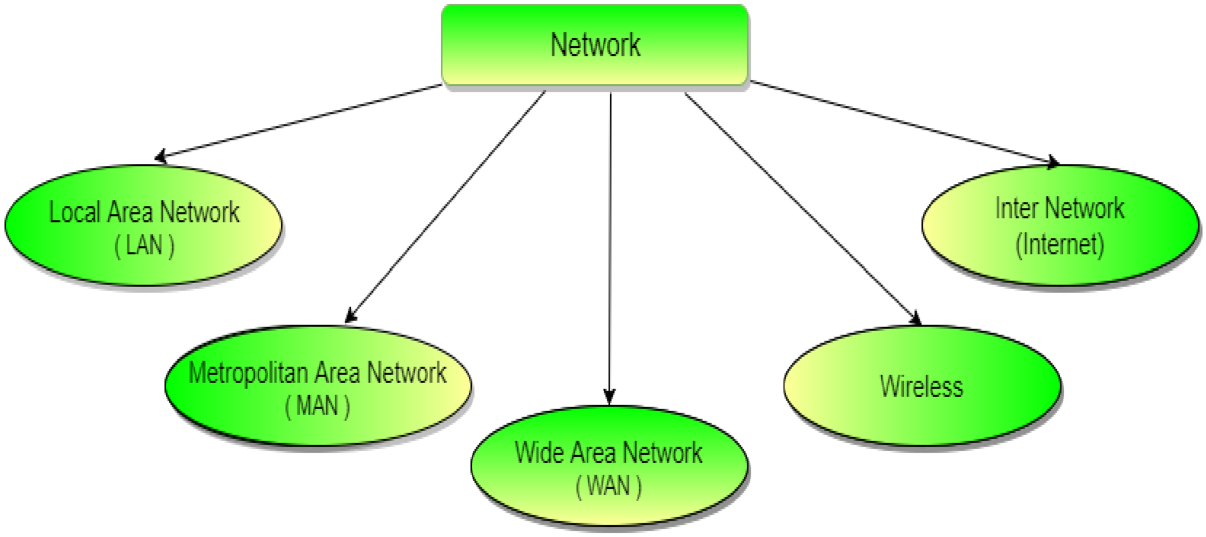
- Improperly installed hardware or software

- Operating systems or firmware that have not been updated
- Misused hardware or software
- Poor or a complete lack of physical security
- Insecure passwords
- Design flaws in a device’s operating system or in the network

Types of Communication Networks

Communication Networks can be of following 5 types:

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)
4. Wireless
5. Inter Network (Internet)

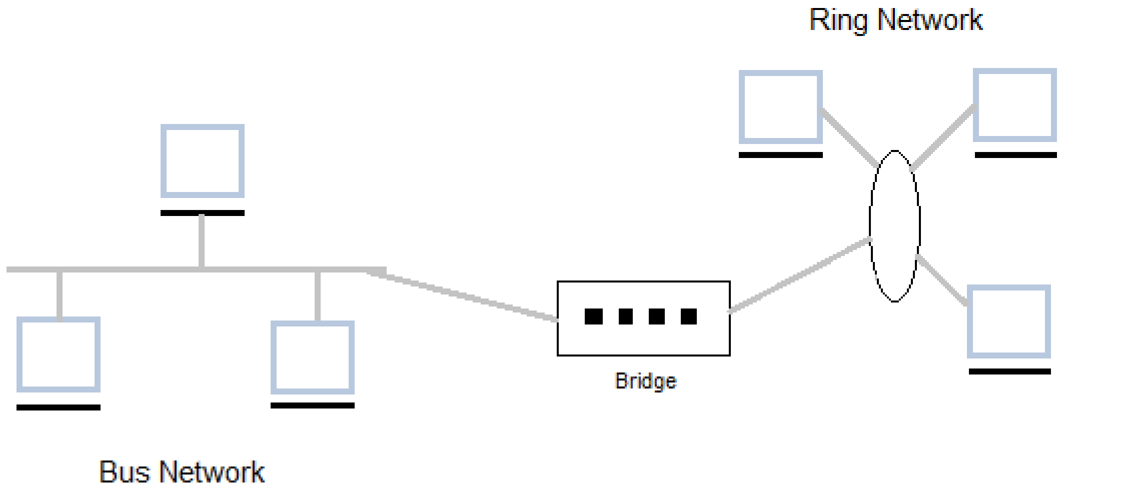

Network
Local Area Network (LAN)
Inter Network (Internet)
Metropolitan Area Network (MAN)
Wireless
Wide Area Network (WAN)

Local Area Network (LAN)

It is also called LAN and designed for small physical areas such as an office, group of buildings or a factory. LANs are used widely as it is easy to design and to troubleshoot. Personal computers and workstations are connected to each other through LANs. We can use different types of topologies through LAN, these are Star, Ring, Bus, Tree etc.

LAN can be a simple network like connecting two computers, to share files and network among each other while it can also be as complex as interconnecting an entire building.

LAN networks are also widely used to share resources like printers, shared hard-drive etc.



(Different Topologies interconnected in a Local Area Network)

Characteristics of LAN

- LAN's are private networks, not subject to tariffs or other regulatory controls.
- LAN's operate at relatively high speed when compared to the typical WAN.
- There are different types of Media Access Control methods in a LAN, the prominent ones are Ethernet, Token ring.
- It connects computers in a single building, block or campus, i.e. they work in a restricted geographical area.

Applications of LAN

- One of the computer in a network can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
- Connecting Locally all the workstations in a building to let them communicate with each other locally without any internet access.
- Sharing common resources like printers etc are some common applications of LAN.

Advantages of LAN

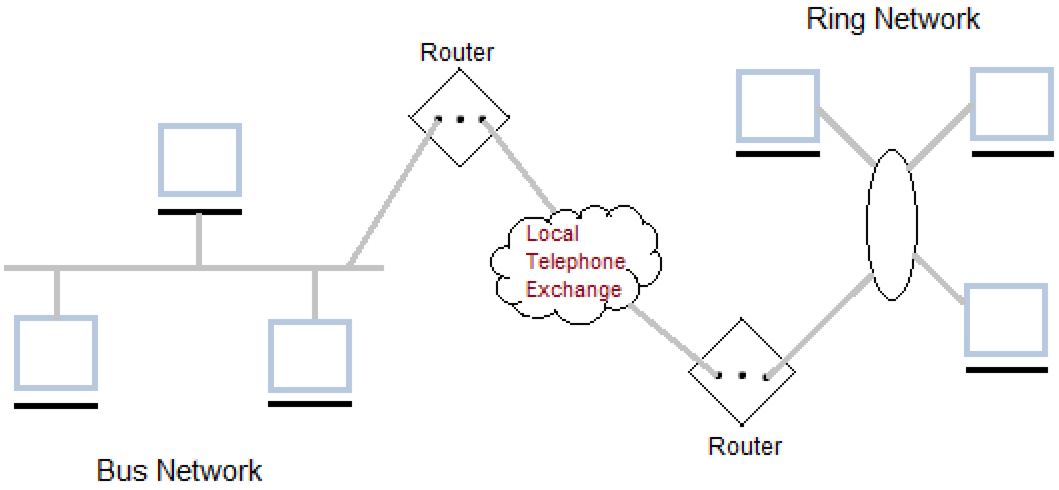
- **Resource Sharing:** Computer resources like printers, modems, DVD-ROM drives and hard disks can be shared with the help of local area networks. This reduces cost and hardware purchases.
- **Software Applications Sharing:** It is cheaper to use same software over network instead of purchasing separate licensed software for each client a network.
- **Easy and Cheap Communication:** Data and messages can easily be transferred over networked computers.
- **Centralized Data:** The data of all network users can be saved on hard disk of the server computer. This will help users to use any workstation in a network to access their data. Because data is not stored on workstations locally.
- **Data Security:** Since, data is stored on server computer centrally, it will be easy to manage data at only one place and the data will be more secure too.
- **Internet Sharing:** Local Area Network provides the facility to share a single internet connection among all the LAN users. In Net Cafes, single internet connection sharing system keeps the internet expenses cheaper.

Disadvantages of LAN

- **High Setup Cost:** Although the LAN will save cost over time due to shared computer resources, but the initial setup costs of installing Local Area Networks is high.
- **Privacy Violations:** The LAN administrator has the rights to check personal data files of each and every LAN user. Moreover he can check the internet history and computer use history of the LAN user.
- **Data Security Threat:** Unauthorized users can access important data of an organization if centralized data repository is not secured properly by the LAN administrator.
- **LAN Maintenance Job:** Local Area Network requires a LAN Administrator because, there are problems of software installations or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is needed at this full time job.
- **Covers Limited Area:** Local Area Network covers a small area like one office, one building or a group of nearby buildings.

Metropolitan Area Network (MAN)

It was developed in 1980s.It is basically a bigger version of LAN. It is also called MAN and uses the similar technology as LAN. It is designed to extend over the entire city. It can be means to connecting a number of LANs into a larger network or it can be a single cable. It is mainly hold and operated by single private company or a public company.



Characteristics of MAN

- It generally covers towns and cities (50 km)
- Communication medium used for MAN are optical fibers, cables etc.
- Data rates adequate for distributed computing applications.

Advantages of MAN

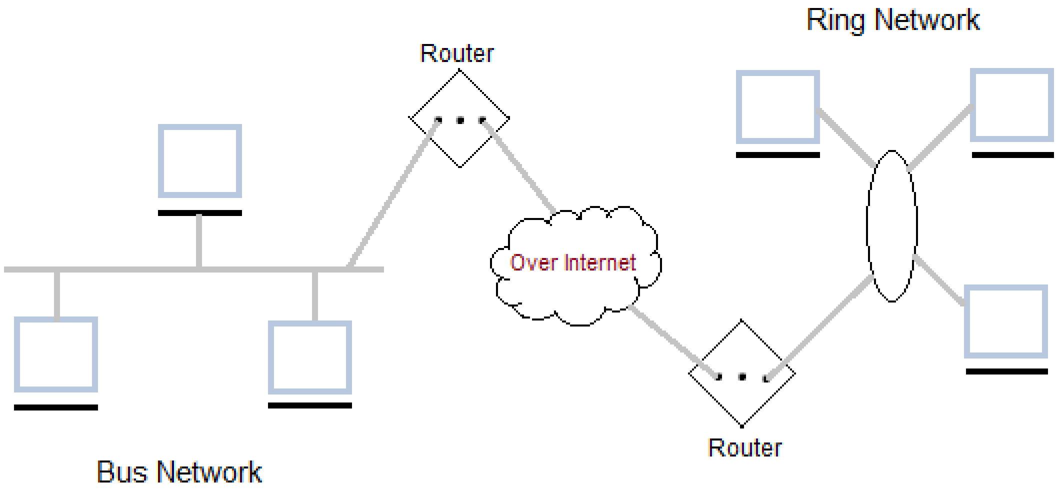
- Extremely efficient and provide fast communication via high-speed carriers, such as fibre optic cables.
- It provides a good back bone for large network and provides greater access to WANs.
- The dual bus used in MAN helps the transmission of data in both directions simultaneously.
- A MAN usually encompasses several blocks of a city or an entire city.

Disadvantages of MAN

- More cable required for a MAN connection from one place to another.
- It is difficult to make the system secure from hackers and industrial espionage(spying) graphical regions.

Wide Area Network (WAN)

It is also called WAN. WAN can be private or it can be public leased network. It is used for the network that covers large distance such as cover states of a country. It is not easy to design and maintain. Communication medium used by WAN are PSTN or Satellite links. WAN operates on low data rates.



Characteristics of WAN

- It generally covers large distances(states, countries, continents).
- Communication medium used are satellite, public telephone networks which are connected by routers.

Advantages of WAN

- Covers a large geographical area so long distance business can connect on the one network.
- Shares software and resources with connecting workstations.
- Messages can be sent very quickly to anyone else on the network. These messages can have picture, sounds or data included with them(called attachments).
- Expensive things(such as printers or phone lines to the internet) can be shared by all the computers on the network without having to buy a different peripheral for each computer.
- Everyone on the network can use the same data. This avoids problems where some users may have older information than others.

Disadvantages of WAN

- Need a good firewall to restrict outsiders from entering and disrupting the network.
- Setting up a network can be an expensive, slow and complicated. The bigger the network the more expensive it is.
- Once set up, maintaining a network is a full-time job which requires network supervisors and technicians to be employed.
- Security is a real issue when many different people have the ability to use information from other computers. Protection against hackers and viruses adds more complexity and expense.

Wireless Network

Digital wireless communication is not a new idea. Earlier, **Morse code** was used to implement wireless networks. Modern digital wireless systems have better performance, but the basic idea is the same.

Wireless Networks can be divided into three main categories:

1. **System interconnection**
2. **Wireless LANs**
3. **Wireless WANs**

System Interconnection

System interconnection is all about interconnecting the components of a computer using **short-range radio**. Some companies got together to design a short-range wireless network called **Bluetooth** to connect various components such as monitor, keyboard, mouse and printer, to the main unit, without wires. Bluetooth also allows digital cameras, headsets, scanners and other devices to connect to a computer by merely being brought within range.

In simplest form, system interconnection networks use the master-slave concept. The system unit is normally the **master**, talking to the mouse, keyboard, etc. as **slaves**.

Wireless LANs

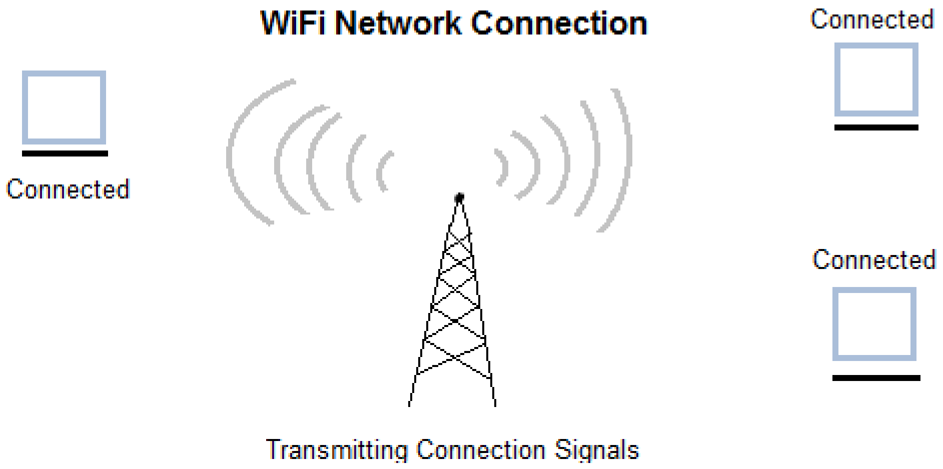
These are the systems in which every computer has a **radio modem** and **antenna** with which it can communicate with other systems. Wireless LANs are becoming increasingly common in small offices and homes, where installing **Ethernet** is considered too much trouble. There is a standard for wireless LANs called **IEEE 802.11**, which most systems implement and which is becoming very widespread.

Wireless WANs

The radio network used for cellular telephones is an example of a low-bandwidth wireless WAN. This system has already gone through three generations.

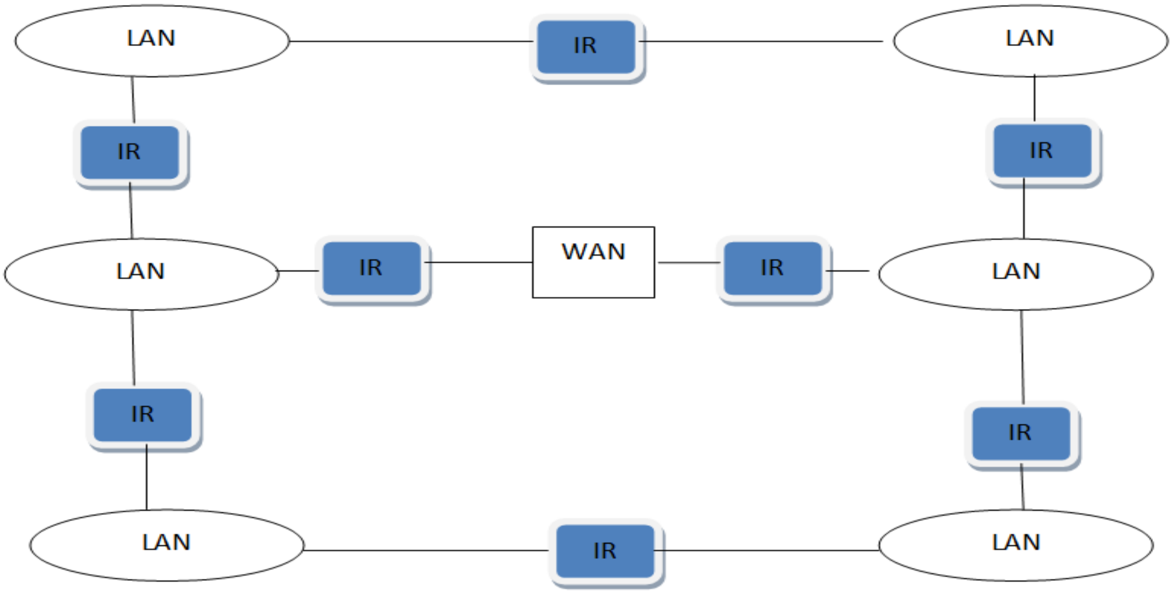
- The first generation was analog and for voice only.
- The second generation was digital and for voice only.

- The third generation is digital and is for both voice and data.



Inter Network

Inter Network or Internet is a combination of two or more networks. Inter network can be formed by joining two or more individual networks by means of various devices such as routers, gateways and bridges.



INTERNETWORK

Computer Network Models

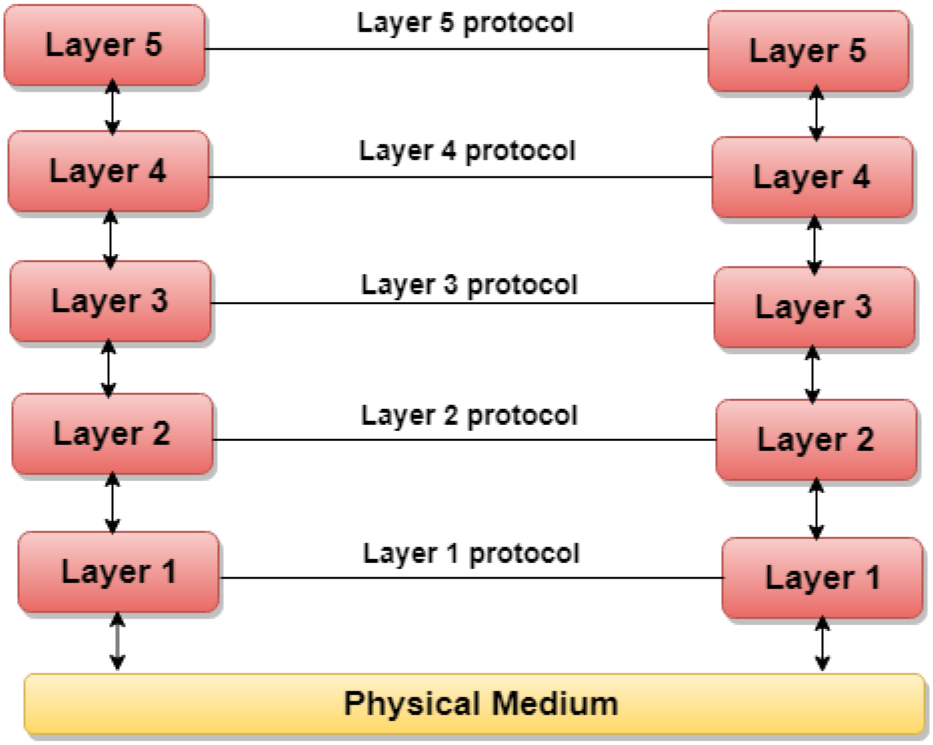
A communication subsystem is a complex piece of Hardware and software. Early attempts for implementing the software for such subsystems were based on a single, complex, unstructured program with many interacting components. The resultant software was very difficult to test and modify. To overcome such problem, the ISO has developed a layered approach. In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task. Therefore, we can say that networking tasks depend upon the layers.

Layered Architecture

- The main aim of the layered architecture is to divide the design into small pieces.
- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.

- The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a higher layer and hiding the details from the layers of how the services are implemented.
- The basic elements of layered architecture are services, protocols, and interfaces.
    - **Service:** It is a set of actions that a layer provides to the higher layer.
    - **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
    - **Interface:** It is a way through which the message is transferred from one layer to another layer.
- In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.

Let's take an example of the five-layered architecture.



- In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which the actual communication takes place.
- In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
- A set of layers and protocols is known as network architecture.

Cyber Security Objectives and Services

Understanding Cyber Security

Cyber security is a complex field that requires a deep understanding of the various threats that exist and the measures that can be taken to protect against them. It is important to understand the different types of threats that exist, such as malware, phishing, and ransomware, and the different types of security measures that can be taken to protect against them. This includes the use of firewalls, antivirus software, and other security measures. It is also important to understand the different types of data that need to be protected, such as customer data, financial data, and intellectual property.

Implementing Cyber Security Measures

Once an organization has a good understanding of the threats that exist and the measures that can be taken to protect against them, it is important to implement the necessary security measures. This includes the use of firewalls, antivirus software, and other security measures. It is also important to ensure that all employees are trained on the proper use of these security measures and that they are aware of the risks associated with not following security protocols. Additionally, organizations should regularly review their security measures to ensure that they are up to date and effective.

Monitoring Cyber Security

In addition to implementing security measures, organizations should also monitor their networks and systems for any suspicious activity. This includes monitoring for any unauthorized access to the network or any suspicious activity on the network. Organizations should also monitor for any changes to the system or any suspicious activity on the system. Additionally, organizations should regularly review their security measures to ensure that they are up to date and effective.

Responding to Cyber Security Incidents

When a cyber security incident occurs, it is important for organizations to respond quickly and effectively. This includes identifying the source of the attack, assessing the damage, and taking steps to mitigate the damage. It is also important to notify the appropriate authorities and take steps to prevent similar incidents from occurring in the future. Additionally, organizations should review their security measures to ensure that they are up to date and effective.

Developing Cyber Security Policies

Organizations should also develop and implement cyber security policies to ensure that their networks and systems are secure. These policies should include guidelines for the use of the network, the use of passwords, and the use of encryption. Additionally, organizations should ensure that all employees are aware of the policies and that they are following them. This includes regularly reviewing the policies and making sure that they are up to date and effective.

Educating Employees on Cyber Security

Organizations should also ensure that all employees are educated on cyber security. This includes providing training on the proper use of the network, the use of passwords, and the use of encryption. Additionally, organizations should ensure that all employees are aware of the risks associated with not following security protocols. This includes regularly reviewing the policies and making sure that they are up to date and effective.

Investing in Cyber Security Solutions

Organizations should also invest in cyber security solutions to ensure that their networks and systems are secure. This includes investing in firewalls, antivirus software, and other security measures. Additionally, organizations should ensure that all employees are aware of the risks associated with not following security protocols. This includes regularly reviewing the security measures to ensure that they are up to date and effective.

Developing a Cyber Security Plan

Organizations should also develop a cyber security plan to ensure that their networks and systems are secure. This plan should include the steps that need to be taken to protect against cyber threats, the steps that need to be taken to respond to cyber security incidents, and the steps that need to be taken to ensure that all employees are aware of the risks associated with not following security protocols. Additionally, organizations should regularly review their security measures to ensure that they are up to date and effective.

common cyber security myths

1. security software slows down or interrupts workflow

this one simply isn’t true, and we believe the myth has originated from poor implementation of security tools, rather than the limitations of the tools themselves. if security tools have been implemented properly then you should be provided with security without affecting your users’ productivity.

2. i have a strong password, i am safe

whilst having a strong password is a necessity, unfortunately it isn’t enough on its own. a good way to add another level of security is to use multi-factor authentication (mfa), requiring users to authenticate themselves via a second method such as their phone or an app like google authenticator. with mfa in place, even if criminals do manage to get hold of usernames and passwords, they still won’t be able log in without the ‘second factor’.

3. security costs too much

companies who think like this are often not considering the downside costs. data breaches will end up being much costlier to your business than making sure you have dedicated security solutions in place before they can happen. capita estimates the average cost of a data breach to be $3.86 million, considering the cost of detecting and escalating a breach, notifying those affected and the regulatory authorities, lost business and reputational damage, and paying fines, legal fees and other costs associated with making things right.

4. i will know straight away if my business is attacked

this rarely the case these days. there used to be some easy signs (pop up ads or slow loading browsers) but scammers have become stealthier. hacking is a silent crime and it is in criminals' best interest to remain unnoticed for as long as possible. the longer they have access to your systems, the more data they can steal.

5. cybersecurity is solely the it department's responsibility

unfortunately, neglectful employees are the number one cause of cybersecurity breaches, so you can't rely solely on the it department to keep your organization secure online – everyone has a role to play. all your staff should be using corporate laptops/tablets/phones with at least 2 factor authentication, as well as ensuring that their installed security software is up to date.

6. cybersecurity threats only come from outside sources

following on from our last point, research suggests that up to 75% of data breaches come from the inside. occasionally this will be a disgruntled employee looking for revenge, but more often than not it is employees who have not been given proper security training or are not following your security protocols.

7. my data isn't important, it's not a big deal if i am hacked

this is an illusion. even if hackers gain only usernames and passwords, this can still result in very bad outcomes for anyone who's data was compromised, as many people use the same credentials for most of their services, including for their online banking.

8. we use apple devices because they can't be hacked

there is a belief that apple products are immune to cyber threats – this isn't the case. apple products can and do get hacked and users who think their devices are invulnerable are more susceptible to data loss.

9. it is easy to spot phishing

phishing is one of the most common ways of stealing people’s personal data or gaining access to a system and usually involves a replica of a known service. it can be so well hidden in an email that anyone could fall prey to it. always be wary of the links you open, and never think that you couldn’t be caught out. make sure that your staff are aware of the risk of phishing. training can help them to understand how sophisticated such scams can be and how easy it is to get caught out.

10. i don’t have a computer, i can’t be hacked

in this day and age, computers are not the only targets for hackers and scammers as so many of our devices connect to the internet. scammers go after phones, routers and even smart tvs. we must make sure we are protecting all end points.

Cybercrime such as ransomware attacks, viruses, scams, theft, email phishing, impersonation, and hacking is increasingly common. The general lack of care and attention towards cyber-security in the online community is owed to several pre-existing myths about online safety.

Here are 5 such misconceptions about cyber-security.

1. Antivirus and Cyber-Security Software is Good Enough

There’s a lot that can go wrong here. Although most people feel at ease after installing security software, they’re not nearly air-tight in reality. The servers of such security software providers are vulnerable to hacking attacks, rendering the clients’ defenses useless.

The kind of cyber-security software you choose is also important. It’s easy to select an antivirus at random and live to regret it later. Always go with reliable providers with stronger safeguards. Some great ones might charge a buck or two, but curtailing costs here might cost you big-time in the future.

2. Complex Passwords Cannot Be Cracked

Passwords are becoming really easy to breach for hackers. Special programs are capable of cracking the longest and most confusing passwords by trying billions of different combinations in the space of seconds. Password trends can also be further replicated to breach your security in multiple online avenues, e.g., having a password for a social media site and using the same one for your email account.

Temporary passwords, OTPs, and two-factor authentication are a way to reduce the risk.

3. My Data Isn’t Worth Anything

That is not true. If it were, social media would never be free to begin with. If a service such as that is free, it monetizes your data instead, selling it to advertisers as an entire ‘customer’ profile.

Data can be materialized for crime, such as theft, impersonation, and physical harm. If it’s valuable for some, it’s valuable for many.

4. Scams and Phishing Are Glaringly Obvious

Phishing schemes and scams are getting more and more intelligent and convincing. Some pretend to withhold your sensitive information via webcam and threaten to release it. Others masquerade as services that you are currently subscribed to and give ‘reminders’ about privacy settings updates.

The data they used to reach you, such as the email address and password, has probably been breached. Some hackers even manage to breach the social media accounts of people you know and use your trust in them against you by sending links to malicious content.

5. Mainstream Websites Are Safe to Visit

All of the big websites employ cookies to track your internet trajectory. Despite the onsite safety, these companies that own the sites possess your data. If any of these companies are hacked, your data is breached too. Consequently, your data isn’t as safe with big websites either.

Bank Accounts Hacked in Nepal

- **Date:** February 3, 2023
- **Attack type:** credential theft
- **Target:** Individuals using net banking
- **Impact:** Several million rupees stolen

Eight malicious actors were arrested in Kathmandu, Nepal, were arrested by the police for hacking into bank accounts. The attackers shared the Android package kit (APK) for a fake app called Nepali Keti over WhatsApp. Then they hacked into the bank accounts of the people who downloaded the app and stole money.

XSS vulnerabilities found in DMS providers

- **Date:** February 7, 2023
- **Attack type:** Zero-day
- **Target:** OnlyOffice, OpenKM, LogicalDOC, Mayan
- **Vulnerability:** Improper input neutralization
- **Impact:** Unknown

Four DMS providers reportedly had XSS vulnerability – CWE – 79. The companies have both free and freemium offerings. The zero-day vulnerabilities were discovered by Rapid7 during a regular inspection.

71 million request-per-second HTTP DDoS attack thwarted by CloudFlare

- **Date:** February 14, 2023
- **Attack type:** DDoS
- **Target:** Cloudflare users
- **Perpetrators:** Unknown
- **Impact:** The attack was mitigated

On 14th February 2023, Cloudflare thwarted the largest known DDoS attack peaking at 71 million requests per second. The attack was mounted against gaming platforms, cryptocurrency companies, and hosting providers, among others, that use Cloudflare to protect their websites. The attack was based on HTTP/2 and involved 30,000 IP addresses.

Dish Network faced a data breach

- **Date:** February 23, 2023
- **Attack type:** Data Breach
- **Target:** Dish Network
- **Impact:** Some data was extracted and Dish’s share price fell by 6.5%

Dish Network, one of the USA’s biggest television providers, disclosed that the network outage reported earlier was connected to a cyber attack. The root causes of the intrusion are yet to be found. The attack resulted in data theft and internal communication breakdown.

US Marshals Service faces ransomware attack

- **Date:** February 17, 2023
- **Attack type:** Ransomware
- **Target:** USMS
- **Impact:** Sensitive law enforcement data exposed

The U.S. Marshals Service is responsible for sensitive tasks like the security of federal judges, fugitive apprehension, etc. The stand-alone USMS system was compromised by attackers exposing data related to USMS investigations.

Major Cyber Attacks in January 2023

In this section, we'll learn about recent cyber attacks – their targets, perpetrators, impact, and current status. This is not an exhaustive list. We've picked the most impactful attacks.

T-Mobile Data Breach

- **Date:** January 5, 2023
- **Attack type:** API data breach
- **Target:** T-Mobile
- **Perpetrator:** Unknown
- **Impact:** Limited types of information were exposed affecting 37 million users

On January 19, 2023, T-Mobile, a wireless telecommunication provider in the US, announced that a bad actor had gained access to some customer data through a vulnerable API. As per their declaration, sensitive data like payment card information, or social security numbers were stolen in the breach.

Attack on AirFrance and KLM

- **Date:** January 9, 2023
- **Attack type:** Data breach
- **Target:** Flying Blue customers of AirFrance and KLM
- **Perpetrator:** Unknown

- **Impact:** Exposure of email IDs, user names, earned miles balance

In a recent report, two major airlines, AirFrance and KLM have confirmed unauthorized access to customer data. The attack exposed some personally identifiable information about Flying Blue customers. However, no Passport, financial information, or social security information was exposed. Flying Blue is a customer-loyalty program run by a number of airlines.

Windows ALPC Zero Day

- **Date:** January 10, 2023
- **Attack type:** Zero-day
- **Target:** Windows Advanced Local Procedure Call
- **CVE**: CVE-2023-21674
- **Impact**: Privilege escalation

According to Microsoft, A malicious user who successfully exploited this vulnerability could gain SYSTEM privileges"

Notably, Microsoft released 98 patches on January 10, 2023, including the one for the ALPC zero-day vulnerability.

Attack on Mailchimp

- **Date:** January 11, 2023
- **Attack type:** Data Breach through social engineering
- **Target:** Tool used by Mailchimp's customer-facing teams
- **Perpetrator:** Unknown
- **Impact:** Unauthorized access to 133 Mailchimp accounts

On January 11, 2023 Mailchimp discovered unauthorized access to some Mailchimp accounts. Attackers used social engineering to steal employee credentials for a tool used by MailChimp's customer-facing employees. As per the declaration by Mailchimp, the attack was limited to 133 accounts. On 12th January the affected accounts were shut down and later reinstated.

A third-party data breach affected Nissan North America

- **Date:** January 16, 2023

- **Attack type:** Third-party data breach
- **Target:** A third-party software development vendor used by Nissan North America
- **Perpetrator:** Unknown individual
- **Impact:** Personally Identifiable Information of 17,998 customers was exposed

Nissan North America reported on January 16, 2023, a data breach that had taken place in June 2022. A third-party vendor that had access to limited customer data for development purposes was victimized by the bad actor. An investigation launched by Nissan in September 2022 confirmed that the attack took advantage of the badly configured database used by the vendor.

Attack on PayPal customers

- **Date:** January 18, 2023
- **Attack type:** Credential stuffing
- **Target:** PayPal customers
- **Perpetrator:** Unknown
- **Impact:** Hackers had access to the personal data of 34,942 PayPal users for 2 days

Credential stuffing is a cyber-attack where hackers use automated tools to enter thousands of user IDs and passwords stolen during earlier attacks into the input fields meant for customers. Due to the habit of people using the same credentials for multiple accounts, credential stuffing actually works.

In the case of PayPal users, hackers had access to the full names, dates of birth, social security numbers, postal addresses, and individual tax identification numbers of 34,942 users for 2 days.

As cyber-attacks volume and complexity increase, cyber security's importance also increases. Cyber security is critical because it helps to protect organizations and individuals from cyber attacks. Cyber security can help to prevent data breaches, identity theft, and other types of cybercrime. Organizations must have strong cyber security measures to protect their data and customers.

1. Technology Innovation

The importance of cyber security regarding technology innovation is that it helps protect ideas and intellectual property from theft or being copied without permission. This is important because it allows companies to maintain a competitive advantage and keep their products and services safe from competitors. Additionally, it helps to ensure that new products and services are not easily replicated or stolen before they can be released to the market.

2. Cloud Transformation

The cloud has transformed how we think about IT, but it has also introduced new security risks. As organizations move more critical data and applications to the cloud, they must know the latest cyber security threats and how to protect themselves.

One of the most significant advantages of the cloud is that it allows organizations to be more agile and responsive to change. However, this agility can also introduce new security risks. For example, a cloud provider may not have the same security controls as a traditional on-premises data center. Cloud data is often spread across multiple physical locations, making protecting it more challenging.

Organizations must be aware of these new risks and take steps to mitigate them. They should work with their cloud providers to ensure that adequate security controls are in place. They should also consider using a cloud security platform to help manage and monitor their cloud environment.

3. Impact on Business Operations

The internet has become a staple in business operations for the majority of companies across the globe. The increase in internet usage has led to a rise in cyber-attacks, which can significantly impact business operations. Cyber security in business helps protect itself against these attacks, including data breaches, phishing scams, and ransom ware. Cyber security can help businesses to protect their data, customers, and reputation.

4. Maintaining Customer and Employee Trust

Customers and employees trust that their information will be protected from cyber threats. To maintain this trust, businesses must invest in cyber security measures to protect customer and employee data. This may include installing firewalls, encrypting data, and creating secure passwords. By taking these steps, businesses can show their commitment to protecting customer and employee information, which can help to build and maintain trust.

5. Securing Financial Position of the Organization

The importance of cyber security to ensure an organization's financial position cannot be understated. In today's interconnected world, where sensitive data is often stored digitally, a breach in security can have disastrous consequences. Not only can it lead to the loss of crucial data, but it can also damage an organization's reputation and bottom line. A cyber attack can result in the loss of customer confidence, increased costs, and a drop in stock value.

In some cases, it can even lead to bankruptcy. For these reasons, organizations need to take steps to protect their data and their systems from attack. It includes investing in cyber security measures such as firewalls, intrusion detection systems, and encryption.

6. Staying Strong Amidst Competition

Cyber security is important to gain competitive advantages because it helps protect businesses and organizations from cyber attacks. By investing in cyber security, businesses can improve their security posture and make it more difficult for attackers to penetrate their systems. As a result, it can give them a competitive edge over companies that have not invested in cyber security. Additionally, businesses that cyber attacks have victimized can use their experience to create better defenses against future attacks and share their knowledge with other companies to help them improve their cyber security.

7. Avoiding Fines and Penalties

The importance of cyber security in avoiding fines and penalties is that it helps protect businesses and individuals from data breaches, cyber-attacks, and other online threats. By implementing strong cyber security measures, companies and individuals can help to safeguard their data and avoid potential fines and penalties.

8. Preserve the Organization's Ability to Function

Organizations face many potential risks regarding their ability to function correctly. One of the most significant risks is a cyber attack. Cyber security is critical because it helps protect organizations from these attacks.

Overall, cyber security is important because it helps protect organizations from the many risks they face. By having strong cyber security measures in place, organizations can reduce the chances of a successful attack and minimize the damage that an attack can cause.

What is a Cyber Attack?

Before heading to the different types of cyber attacks, we will first walk you through a cyber attack. When there is an unauthorized system/network access by a third party, we term it as a cyber attack. The person who carries out a cyber attack is termed as a hacker/attacker.

Cyber-attacks have several negative effects. When an attack is carried out, it can lead to data breaches, resulting in data loss or data manipulation. Organizations incur financial losses, customer trust gets hampered, and there is reputational damage. To put a curb on cyber attacks, we implement cyber security. Cyber security is the method of safeguarding networks, computer systems, and their components from unauthorized digital access.

The COVID-19 situation has also had an adverse impact on cyber security. According to Interpol and WHO, there has been a notable increase in the number of cyberattacks during the COVID-19 pandemic.

Different types of cyber attacks.

Life today has become far more comfortable because of various digital devices and the internet to support them. There is a flip side to everything good, and that also applies to the digital world today. The internet has brought in a positive change in our lives today, but with that, there is also an enormous challenge in protecting your data. This gives rise to cyber attacks. In this article, we will discuss the different types of cyber attacks and how they can be prevented.

What is a Cyber Attack?

Before heading to the different types of cyber attacks, we will first walk you through a cyber attack. When there is an unauthorized system/network access by a third party, we term it as a cyber attack. The person who carries out a cyber attack is termed as a hacker/attacker.

Cyber-attacks have several negative effects. When an attack is carried out, it can lead to data breaches, resulting in data loss or data manipulation. Organizations incur financial losses, customer trust gets hampered, and there is reputational damage. To put a curb on cyber attacks, we implement cyber security. Cyber security is the method of safeguarding networks, computer systems, and their components from unauthorized digital access.

The COVID-19 situation has also had an adverse impact on cyber security. According to Interpol and WHO, there has been a notable increase in the number of cyber attacks during the COVID-19 pandemic.

Now that you know what a cyber attack is, let look at the different types of cyber attacks.

How Often Do Cyber Attacks Occur?

Cyber attacks are becoming increasingly common in our modern digital world. They can cause severe damage to individuals, businesses, and governments. People launch cyber attacks for several reasons, including financial gain, espionage, activism, and sabotage. In addition, hackers may launch attacks simply for the challenge or to prove their skills.

Why Do People Launch Cyber Attacks?

There are many reasons why people launch cyber attacks, including financial gain, espionage, activism, and sabotage. In some cases, cyber-attacks may be politically motivated to cause damage to their opponents.

What Happens During a Cyber Attack?

During a cyber attack, the attacker gains unauthorized access to a computer system, network, or device for stealing, modifying, or destroying data. The attacker may use a variety of tactics, including malware, social engineering, or exploiting vulnerabilities in software or systems.

How Do Cyber Attacks Happen?

Cyber attacks can happen in various methods. For instance, a hacker can use phishing methods to trick a user into clicking a malicious link or entering their login credentials into a fake website. Alternatively, a hacker may cause damage to the vulnerability in the software to access other devices to steal sensitive information.

Types of Cyber Attacks

There are many varieties of cyber attacks that happen in the world today. If we know the various types of cyber attacks, it becomes easier for us to protect our networks and systems against them. Here, we will closely examine the top ten cyber-attacks that can affect an individual, or a large business, depending on the scale.

Let’s start with the different types of cyber attacks on our list:

1. Malware Attack

This is one of the most common types of cyber attacks. “Malware” refers to malicious software viruses including worms, spyware, ransom ware, adware, and Trojans.

The trojan virus disguises itself as legitimate software. Ransom ware blocks access to the network's key components, whereas Spyware is software that steals all your confidential data without your knowledge. Adware is software that displays advertising content such as banners on a user's screen.

Malware breaches a network through a vulnerability. When the user clicks a dangerous link, it downloads an email attachment or when an infected pen drive is used.

Let’s now look at how we can prevent a malware attack:

- Use antivirus software. It can protect your computer against malware. Avast Antivirus, Norton Antivirus, and McAfee Antivirus are a few of the popular antivirus software.
- Use firewalls. Firewalls filter the traffic that may enter your device. Windows and Mac OS X have their default built-in firewalls, named Windows Firewall and Mac Firewall.
- Stay alert and avoid clicking on suspicious links.
- Update your OS and browsers, regularly.

2. Phishing Attack

Phishing attacks are one of the most prominent widespread types of cyber attacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake mails.

Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment. By doing so, attackers gain access to confidential information and account credentials. They can also install malware through a phishing attack.

Phishing attacks can be prevented by following the below-mentioned steps:

- Scrutinize the emails you receive. Most phishing emails have significant errors like spelling mistakes and format changes from that of legitimate sources.
- Make use of an anti-phishing toolbar.
- Update your passwords regularly.

3. Password Attack

It is a form of attack wherein a hacker cracks your password with various programs and password cracking tools like Air crack, Cain, Abel, John the Ripper, Hash cat, etc. There are different types of password attacks like brute force attacks, dictionary attacks, and keylogger attacks.

Listed below are a few ways to prevent password attacks:

- Use strong alphanumeric passwords with special characters.
- Abstain from using the same password for multiple websites or accounts.
- Update your passwords; this will limit your exposure to a password attack.
- Do not have any password hints in the open.

4. Man-in-the-Middle Attack

A Man-in-the-Middle Attack (MITM) is also known as an eavesdropping attack. In this attack, an attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data.

As seen below, the client-server communication has been cut off, and instead, the communication line goes through the hacker.

MITM attacks can be prevented by following the below-mentioned steps:

- Be mindful of the security of the website you are using. Use encryption on your devices.
- Refrain from using public Wi-Fi networks.

5. SQL Injection Attack

A Structured Query Language (SQL) injection attack occurs on a database-driven website when the hacker manipulates a standard SQL query. It is carried by injecting a malicious code into a vulnerable website search box, thereby making the server reveal crucial information.

This results in the attacker being able to view, edit, and delete tables in the databases. Attackers can also get administrative rights through this.

To prevent a SQL injection attack:

- Use an Intrusion detection system, as they design it to detect unauthorized access to a network.
- Carry out a validation of the user-supplied data. With a validation process, it keeps the user input in check.

6. Denial-of-Service Attack

A Denial-of-Service Attack is a significant threat to companies. Here, attackers target systems, servers, or networks and flood them with traffic to exhaust their resources and bandwidth.

When this happens, catering to the incoming requests becomes overwhelming for the servers, resulting in the website it hosts either shut down or slow down. This leaves the legitimate service requests unattended.

It is also known as a DDoS (Distributed Denial-of-Service) attack when attackers use multiple compromised systems to launch this attack.

Let’s now look at how to prevent a DDoS attack:

- Run a traffic analysis to identify malicious traffic.
- Understand the warning signs like network slowdown, intermittent website shutdowns, etc. At such times, the organization must take the necessary steps without delay.
- Formulate an incident response plan, have a checklist and make sure your team and data center can handle a DDoS attack.
- Outsource DDoS prevention to cloud-based service providers.

7. Insider Threat

As the name suggests, an insider threat does not involve a third party but an insider. In such a case; it could be an individual from within the organization who knows everything about the organization. Insider threats have the potential to cause tremendous damages.

Insider threats are rampant in small businesses, as the staff there hold access to multiple accounts with data. Reasons for this form of an attack are many, it can be greed, malice, or even carelessness. Insider threats are hard to predict and hence tricky.

To prevent the insider threat attack:

- Organizations should have a good culture of security awareness.
- Companies must limit the IT resources staff can have access to depending on their job roles.
- Organizations must train employees to spot insider threats. This will help employees understand when a hacker has manipulated or is attempting to misuse the organization's data.