The Process of Development of Information System: A Typical Software Development Life Cycle

The process of development of information systems in an organization may vary from case to case but ideally the stages of development can be clearly demarcated. The process of development of information system involves the following stages:

1. **Planning-**planning is required as without planning the outcome will be below expectations. Planning sets the objectives of the system in clear and unambiguous terms so that the developer may conform to a well laid set of deliverables rather than a high-sounding statement that may mean little to him. Planning also enables the development process to be structured so that logical methodology is used rather than working in fits and starts. It ensures user participation and helps in greater acceptability and a better outcome from the development process. It leads to a system that is well balanced in both the managerial and technical aspects.
2. **Analysis-**is an activity of technical representation of a system. Over the years many methods have been developed of which the structured analysis and object oriented analysis are most widely used. This step or activity is the first technical representation in abstract terms of the system.
3. **Design-**is the stage where the model or representation of an entity or a system is done (in detail). It is based on the idea that the developer will be able to develop a working system conforming to all the specifications of the design document which would satisfy the user. ·It is a concept which has been borrowed from other branches in engineering where the blueprint of a system or entity to be built later is first created on a piece of paper or digitally to help developers in conceptualization of the system and to understand the specifications of the system.
4. **Coding-**is the actual stage of writing codes to develop the application software according to the specifications as set by the design document. The programming done at this stage to build the system is dictated by the needs of the design specifications. The programmer cannot go beyond the design document.
5. **Testing-**is the testing of the system to check if the application is as per the set specification and to check whether the system will be able to function under actual load of data. The testing is also done to remove any bugs or errors in the code.
6. **Implementation-**is the stage when the system is deployed in the organization. This is a process which often is a difficult one as it involves some customization of the code to fit context specific information in the system.

What is Information Security?

Information Security is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electronic one. Information can be anything like Your details or we can say your profile on social media, your data in mobile phone, your biometrics etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc.

During First World War, Multi-tier Classification System was developed keeping in mind sensitivity of information. With the beginning of Second World War formal alignment of Classification System was done. Alan Turing was the one who successfully decrypted Enigma Machine which was used by Germans to encrypt warfare data.

Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

1. **Confidentiality** – means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.
2. **Integrity** – means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.
3. **Availability** – means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management. Denial of service attack is one of the factor that can hamper the availability of information.

Apart from this there is one more principle that governs information security programs. This is Non repudiation.

- **Non repudiation** – means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. For example in cryptography it is sufficient to show that message matches the digital signature signed with sender's private key and that sender could have a sent a message and nobody else could have altered it in transit. Data Integrity and Authenticity are pre-requisites for Non repudiation.

- **Authenticity** – means verifying that users are who they say they are and that each input arriving at destination is from a trusted source.This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission. For example if take above example sender sends the message along with digital signature which was generated using the hash value of message and private key. Now at the receiver side this digital signature is decrypted using the public key generating a hash value and message is again hashed to generate the hash value. If the 2 value matches then it is known as valid transmission with the authentic or we say genuine message received at the recipient side

- **Accountability** – means that it should be possible to trace actions of an entity uniquely to that entity. For example as we discussed in Integrity section Not every employee should be allowed to do changes in other employees data. For this there is a separate department in an organization that is responsible for making such changes and when they receive request for a change then that letter must be signed by higher authority for example Director of college and person that is allotted that change will be able to do change after verifying his bio metrics, thus timestamp with the user(doing changes) details get recorded. Thus we can say if a change goes like this then it will be possible to trace the actions uniquely to an entity.

At the core of Information Security is Information Assurance, which means the act of maintaining CIA of information, ensuring that information is not compromised in any way when critical issues arise. These issues are not limited to natural disasters, computer/server malfunctions etc.

Thus, the field of information security has grown and evolved significantly in recent years. It offers many areas for specialization, including securing networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning etc.

Difference between Cyber Security and Information Security

The terms **Cyber Security** and Information Security are often used interchangeably. As they both are responsible for the security and protecting the computer system from threats and information breaches and often Cybersecurity and information security are so closely linked that they may seem synonymous and unfortunately, they are used synonymously. If we talk about data security it's all about securing the data from malicious users and threats. Now another question is what is the difference between Data and Information? So one important point is that "not every data can be information" data can be informed if it is interpreted in a context and given meaning. for example **"100798"** is data and if we know that it's the date of birth of a person then it is information because it has some meaning. so information means data that has some meaning.

Examples and Inclusion of Cyber Security are as follows:

- Network Security
- Application Security
- Cloud Security
- Critical Infrastructure

Examples and inclusion of Information Security are as follows:

- Procedural Controls
- Access Controls

- *Technical Controls*
- *Compliance Controls*

Parameters	CYBER SECURITY	INFORMATION SECURITY
Basic Definition	It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.
Protect	It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with the protection of data from any form of threat.
Scope	Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Threat	Cybersecurity deals with the danger in cyberspace.	Information security deals with the protection of data from any form of threat.
Attacks	Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.	Information security strikes against unauthorized access, disclosure modification, and disruption.
Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.

Parameters	CYBER SECURITY	INFORMATION SECURITY
Defense	Acts as first line of defense.	Comes into play when security is breached.

Need Of Information Security

Information system means to consider available countermeasures or controls stimulated through uncovered vulnerabilities and identify an area where more work is needed. The purpose of data security management is to make sure business continuity and scale back business injury by preventing and minimizing the impact of security incidents. The basic principle of Information Security is:

- Confidentially
- Authentication
- Non-Repudiation
- Integrity

The need for Information security:

1. **Protecting the functionality of the organization:**
   The decision maker in organizations must set policy and operates their organization in compliance with the complex, shifting legislation, efficient and capable applications.
2. **Enabling the safe operation of applications:**
   The organization is under immense pressure to acquire and operates integrated, efficient and capable applications. The modern organization needs to create an environment that safeguards application using the organizations IT systems, particularly those application that serves as important elements of the infrastructure of the organization.
3. **Protecting the data that the organization collect and use:**
   Data in the organization can be in two forms are either in rest or in motion, the motion of data signifies that data is currently used or processed by the system. The values of the data motivated the attackers to steal or corrupts the data. This is essential for the integrity and the values of the organization's data. Information security ensures the protection of both data in motion as well as data in rest.
4. **Safeguarding technology assets in organizations:**
   The organization must add intrastate services based on the size and scope of the organization. Organizational growth could lead to the need for public key infrastructure, PKI an integrated system of the software, encryption methodologies. The information security mechanism used by large organizations is complex in comparison to a small organization. The small organization generally prefers symmetric key encryption of data.

Threats to Information Security

Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

Software attacks means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behaves differently.

Malware is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:

1. Infection Methods
2. Malware Actions

Malware on the **basis of Infection** Method are following:

1. **Virus –** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
2. **Worms –** Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network-aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will, for example, consume hard disk space thus slowing down the computer.
3. **Trojan –** The Concept of Trojan is completely different from the viruses and worms. The name Trojan is derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.

Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed.

4.

They often provide backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission. Examples include FTP Trojans, Proxy Trojans, Remote Access Trojans etc.

5.
6. **Bots –**: can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need for human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called **Botnet.**

Malware on the **basis of Actions**:

1. **Adware** – Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer's desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
2. **Spyware** – It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they install themselves and sits silently to avoid detection.

One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.

3.
4. **Ransomware** – It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.
5. **Scareware** – It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.
6. **Rootkits** – are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.
7. **Zombies** – They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.

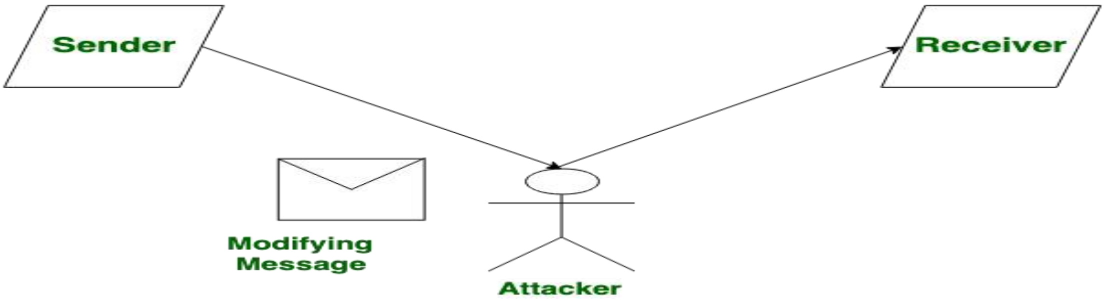
- **Theft of intellectual property** means violation of intellectual property rights like copyrights, patents etc.
- **Identity theft** means to act someone else to obtain person's personal information or to access vital information they have like accessing the computer or social media account of a person by login into the account by using their login credentials.
- **Theft of equipment and information** is increasing these days due to the mobile nature of devices and increasing information capacity.
- **Sabotage** means destroying company's website to cause loss of confidence on part of its customer.
- **Information extortion** means theft of company's property or information to receive payment in exchange. For example ransomware may lock victims file making them inaccessible thus forcing victim to make payment in exchange. Only after payment victim's files will be unlocked.

These are the old generation attacks that continue these days also with advancement every year. Apart from these there are many other threats. Below is the brief description of these new generation threats.

- **Technology with weak security** – With the advancement in technology, with every passing day a new gadget is being released in the market. But very few are fully secured and follows Information Security principles. Since the market is very competitive Security factor is compromised to make device more up to date. This leads to theft of data/ information from the devices
- **Social media attacks** – In this cyber criminals identify and infect a cluster of websites that persons of a particular organization visit, to steal information.
- **Mobile Malware** –There is a saying when there is a connectivity to Internet there will be danger to Security. Same goes for Mobile phones where gaming applications are designed to lure customer to download the game and unintentionally they will install malware or virus on the device.
- **Outdated Security Software** – With new threats emerging everyday, updation in security software is a prerequisite to have a fully secured environment.
- **Corporate data on personal devices** – These days every organization follows a rule BYOD. BYOD means Bring your own device like Laptops, Tablets to the workplace. Clearly BYOD pose a serious threat to security of data but due to productivity issues organizations are arguing to adopt this.
- **Social Engineering** – is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These criminals can trick you into giving your private and confidential information or they will gain your trust to get access to your computer to install a malicious software- that will give them control of your computer. For example email or message from your friend, that was probably not sent by your friend. Criminal can access your friends device and then by accessing the contact list, he can send infected email and message to all contacts. Since the message/ email is from a known person recipient will definitely check the link or attachment in the message, thus unintentionally infecting the computer.

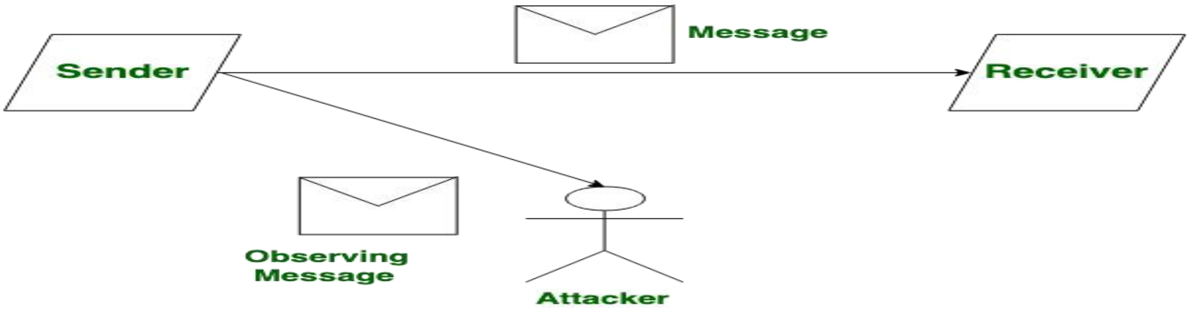
Difference between Active Attack and Passive Attack

Active Attacks: Active attacks are the type of attacks in which, The attacker efforts to change or modify the content of messages. Active Attack is danger for Integrity as well as availability. Due to active attack system is always damaged and System resources can be changed. The most important thing is that, In active attack, Victim gets informed about the attack.



Active Attack

Passive Attacks: Passive Attacks are the type of attacks in which, The attacker observes the content of messages or copy the content of messages. Passive Attack is a danger for Confidentiality. Due to passive attack, there is no any harm to the system. The most important thing is that In passive attack, Victim does not get informed about the attack.



Passive Attack

Active Attack	Passive Attack
In an active attack, Modification in information takes place.	While in passive attack, Modification in the information does not take place.
Active Attack is a danger to **Integrity** as well as **availability**.	Passive Attack is a danger to **Confidentiality**.
In an active attack, attention is on prevention.	While in passive attack attention is on detection.
Due to active attacks, the execution system is always damaged.	While due to passive attack, there is no harm to the system.
In an active attack, Victim gets informed about the attack.	While in a passive attack, Victim does not get informed about the attack.
In an active attack, System resources can be changed.	While in passive attack, System resources are not changing.

Active Attack	Passive Attack
Active attack influences the services of the system.	While in passive attack, information and messages in the system or network are acquired.
In an active attack, information collected through passive attacks are used during executing.	While passive attacks are performed by collecting information such as passwords, and messages by themselves.
Active attack is tough to restrict from entering systems or networks.	Passive Attack is easy to prohibited in comparison to active attack.
Can be easily detected.	Very difficult to detect.

Information Assurance Model in Cyber Security

Information Assurance concerns implementation of methods that focused on protecting and safeguarding critical information and relevant information systems by assuring confidentiality, integrity, availability, and non-repudiation. It is strategic approach focused which focuses more on deployment of policies rather than building infrastructures.

Information Assurance Model :

The security model is multidimensional model based on four dimensions :

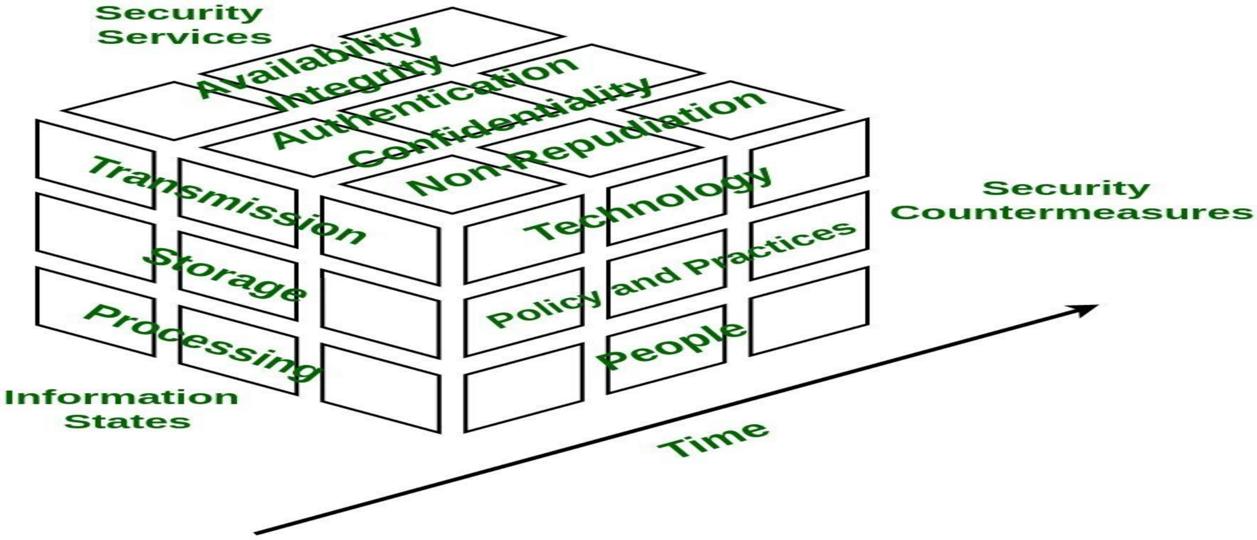
1. **Information States –**
   Information is referred to as interpretation of data which can be found in three states stored, processed, or transmitted.

2. **Security Services –**
   It is fundamental pillar of the model which provides security to system and consists of five services namely availability, integrity, confidentiality, authentication, and non-repudiation.

3. **Security Countermeasures –**
   This dimension has functionalities to save system from immediate vulnerability by accounting for technology, policy & practice, and people.

4. **Time –**
   This dimension can be viewed in many ways. At any given time data may be available offline or online, information and system might be in flux thus, introducing risk of unauthorized access. Therefore, in every phase of System Development Cycle, every aspect of Information Assurance model must be well defined and well implemented in order to minimize risk of unauthorized

access.



Information States :

1. **Transmission –**

   It defines time wherein data is between processing steps.

Example :

In transit over networks when user sends email to reader, including memory and storage encountered during delivery.

2. **Storage –**

   It defines time during which data is saved on medium such as hard drive.Example: Saving document on file server's disk by user.

3. **Processing –**

   It defines time during which data is in processing state.

Example :

Data is processed in random access memory (RAM) of workstation.

4.

Security Services :

1. **Confidentiality –**

   It assures that information of system is not disclosed to unauthorized access and is read and interpreted only by persons authorized to do so. Protection of confidentiality prevents malicious access and accidental disclosure of information. Information that is considered to be confidential is called as **sensitive information**.

To ensure confidentiality data is categorized into different categories according to damage severity and then accordingly strict measures are taken.

Example :

Protecting email content to read by only desired set of users. This can be insured by data encryption. Two-factor authentication, strong passwords, security tokens, and biometric verification are some popular norms for authentication users to access sensitive data.

2. **Integrity –**

   It ensures that sensitive data is accurate and trustworthy and can not be created, changed, or deleted without proper authorization. Maintaining integrity involves modification or destruction of information by unauthorized access.

To ensure integrity backups should be planned and implemented in order to restore any affected data in case of security breach. Besides this cryptographic checksum can also be used for verification of data.

Example :

Implementation of measures to verify that e-mail content was not modified in transit. This can be achieved by using cryptography which will ensure that intended user receives correct and accurate information.

3. **Availability –**

   It guarantees reliable and constant access to sensitive data only by authorized users. It involves measures to sustain access to data in spite of system failures and sources of interference.

To ensure availability of corrupted data must be eliminated, recovery time must be speed up and physical infrastructure must be improved.

Example :

Accessing and throughput of e-mail service.

4. **Authentication –**

   It is security service that is designed to establish validity of transmission of message by verification of individual's identity to receive specific category of information.

To ensure availability of various single factors and multi-factor authentication methods are used. A single factor authentication method uses single parameter to verify users' identity whereas two-factor authentication uses multiple factors to verify user's identity.

Example :

Entering username and password when we log in to website is example of authentication. Entering correct login information lets website verify our identity and ensures that only we access sensitive information.

5. **Non-Repudiation –**

   It is mechanism to ensure sender or receiver cannot deny fact that they are part of data transmission. When sender sends data to receiver, it receives delivery confirmation. When receiver receives message it has all information attached within message regarding sender.

Example :

A common example is sending SMS from one mobile phone to another. After message is received confirmation message is displayed that receiver has received message. In return, message received by receiver contains all information about sender.

Security Countermeasures :

1. **People –**

   People are heart of information system. Administrators and users of information systems must follow policies and practice for designing good system. They must be informed regularly regarding information system and ready to act appropriately to safeguard system.

2. **Policy & Practice –**

   Every organization has some set of rules defined in form of policies that must be followed by every individual working in organization. These policies must be practiced in order to properly handle sensitive information whenever system gets compromised.

3. **Technology –**

   Appropriate technology such as firewalls, routers, and intrusion detection must be used in order to defend system from vulnerabilities, threats. The technology used must facilitate quick response whenever information security gets compromised.

What is Cyber Security?

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called **electronic information security** or **information technology security**.

Types of Cyber Security

Every organization's assets are the combinations of a variety of different systems. These systems have a strong cybersecurity posture that requires coordinated efforts across all of its systems. Therefore, we can categorize cybersecurity in the following sub-domains:

- **Network Security:** It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats.
- **Application Security:** It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks. Successful security begins in the design stage, writing source code, validation, threat modeling, etc., before a program or device is deployed.
- **Information or Data Security:** It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.
- **Identity management:** It deals with the procedure for determining the level of access that each individual has within an organization.
- **Operational Security:** It involves processing and making decisions on handling and securing data assets.
- **Mobile Security:** It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.
- **Cloud Security:** It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.

- **Disaster Recovery and Business Continuity Planning:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.
- **User Education:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.

Classification of Cyber Crime:

1. **Cyber Terrorism –**

   Cyber terrorism is the use of the computer and internet to perform violent acts that result in loss of life. This may include different type of activities either by software or hardware for threatening life of citizens.

   In general, Cyber terrorism can be defined as an act of terrorism committed through the use of cyberspace or computer resources.

2. **Cyber Extortion –**

   Cyber extortion occurs when a website, e-mail server or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand huge money in return for assurance to stop the attacks and to offer protection.

3. **Cyber Warfare –**

   Cyber warfare is the use or targeting in a battle space or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations concerning to the threat of cyber attacks, espionage and sabotage.

4. **Internet Fraud –**

   Internet fraud is a type of fraud or deceit which makes use of the Internet and could include hiding of information or providing incorrect information for the purpose of deceiving victims for money or property. Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace.

5. **Cyber Stalking –**

   This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. In this case, these stalkers know their victims and instead of offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Prevention of Cyber Crime:

Below are some points by means of which we can prevent cyber crime:

1. **Use strong password –**
Maintain different password and username combinations for each account and resist the temptation to write them down. Weak passwords can be easily cracked using certain attacking methods like Brute force attack, Rainbow table attack etc, So make them complex. That means combination of letters, numbers and special characters.

2. **Use trusted antivirus in devices –**
Always use trustworthy and highly advanced antivirus software in mobile and personal computers. This leads to the prevention of different virus attack on devices.

3. **Keep social media private –**
Always keep your social media accounts data privacy only to your friends. Also make sure only to make friend who are known to you.

4. **Keep your device software updated –**
Whenever your get the updates of the system software update it at the same time because sometimes the previous version can be easily attacked.

5. **Use secure network –**
Public Wi-Fi are vulnerable. Avoid conducting financial or corporate transactions on these networks.

6. **Never open attachments in spam emails –**
A computer get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

7. **Software should be updated –** Operating system should be updated regularly when it comes to internet security. This can become a potential threat when cybercriminals exploit flaws in the system.

Cyber Security Tools

Protecting our IT environment is very critical. Every organization needs to take cybersecurity very seriously. There are numbers of hacking attacks which affecting businesses of all sizes. Hackers, malware, viruses are some of the real security threats in the virtual world. It is essential that every company is aware of the dangerous security attacks and it is necessary to keep themselves secure. There are many different aspects of the cyber defence may need to be considered. Here are six essential tools and services that every organization needs to consider to ensure their cybersecurity is as strong as possible. They are described below:

Firewalls
Antivirus Software
PKI Services
MDR Services
Penetration Testing
Staff Training

Cyber Security Tools

3. PKI Services

PKI stands for Public Key Infrastructure. This tool supports the distribution and identification of public encryption keys. It enables users and computer systems to securely exchange data over the internet and verify the identity of the other party. We can also exchange sensitive information without PKI, but in that case, there would be no assurance of the authentication of the other party.

PKI can also be used to:

- Enable Multi-Factor Authentication and access control
- Create compliant, Trusted Digital Signatures.
- Encrypt email communications and authenticate the sender's identity.
- Digitally sign and protect the code.
- Build identity and trust into IoT ecosystems.

4. Managed Detection and Response Service (MDR)

Today's cybercriminals and hackers used more advanced techniques and software to breach organization security So, there is a necessity for every businesses to be used more powerful forms of defences of cybersecurity. MDR is an advanced security service that provides threat hunting, threat intelligence, security monitoring, incident analysis, and incident response. It is a service that arises from the need for organizations (who has a lack of resources) to be more aware of risks and improve their ability to detect and respond to threats. MDR also uses Artificial Intelligence and machine learning to investigate, auto detect threats, and orchestrate response for faster result.

The managed detection and response has the following characteristics:

- Managed detection and response is focused on threat detection, rather than compliance.
- MDR relies heavily on security event management and advanced analytics.
- While some automation is used, MDR also involves humans to monitor our network.
- MDR service providers also perform incident validation and remote response.

5. Penetration Testing

Penetration testing, or pen-test, is an important way to evaluate our business's security systems and security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities exist in operating systems, services and application, improper configurations or risky end-user behavior. In Penetration testing, cybersecurity professionals will use the same techniques and processes utilized by criminal hackers to check for potential threats and areas of weakness.

A pen test attempts the kind of attack a business might face from criminal hackers such as password cracking, code injection, and phishing. It involves a simulated real-world attack on a network or application. This tests can be performed by using manual or automated technologies to systematically evaluate servers, web applications, network devices, endpoints, wireless networks, mobile devices and other potential points of vulnerabilities. Once the pen test has successfully taken place, the testers will present us with their findings threats and can help by recommending potential changes to our system.

6. Staff Training

Staff training is not a 'cybersecurity tool' but ultimately, having knowledgeable employees who understand the cybersecurity which is one of the strongest forms of defence against cyber-attacks. Today's many training tools available that can educate company's staff about the best cybersecurity practices. Every business can organize these training tools to educate their employee who can understand their role in cybersecurity.