**UNIT-I**

**Cyber Security Introduction - Cyber Security Basics:**

Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

**What is cyber security?**

"Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

OR

Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

The term cyber security refers to techniques and practices designed to protect digital data.

The data that is stored, transmitted or used on an information system.

OR

Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks. It is made up of two words one is cyber and other is security

1. Cyber is related to the technology which contains systems, network and programs or data.
2. Whereas security related to the protection which includes systems security, network security and application and information security.

**Why is cyber security important?**

Listed below are the reasons why cyber security is so important in what’s become a predominant digital world:

1. Cyber attacks can be extremely expensive for businesses to endure.
2. In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
3. Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.
4. Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

Because of the above reasons, cyber security has become an important part of the business and the focus now is on developing appropriate response plans that minimize the damage in the event of a cyber attack. But, an organization or an individual can develop a proper response plan only when he has a good grip on cyber security fundamentals.

**Cyber security Fundamentals – Confidentiality:**

Confidentiality is about preventing the disclosure of data to unauthorized parties.

It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous.

Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle (MITM) attacks, disclosing sensitive data.

Standard measures to establish confidentiality include:

1. Data encryption
2. Two-factor authentication
3. Biometric verification
4. Security tokens

**Integrity**

Integrity refers to protecting information from being modified by unauthorized parties.

Standard measures to guarantee integrity include:

1. Cryptographic checksums
2. Using file permissions
3. Uninterrupted power supplies
4. Data backups

**Availability**

Availability is making sure that authorized parties are able to access the information when needed.

Standard measures to guarantee availability include:

1. Backing up data to external drives
2. Implementing firewalls
3. Having backup power supplies
4. Data redundancy

**Types of Cyber Attacks**

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Cyber-attacks can be classified into the following categories:

1. Web-based attacks
2. System-based attacks

**Web-based attacks**

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows

1. **Injection attacks** It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

1. **DNS Spoofing** DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.
2. **Session Hijacking** It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.
3. **Phishing** Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.
4. **Brute force** It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security
5. **Denial of Service** It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following

**Volume-based attacks-**Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

**Protocol attacks-** It consumes actual server resources, and is measured in a packet.

**Application layer attacks-** Its goal is to crash the web server and is measured in request per second.

1. **Dictionary attacks** This type of attack stored the list of a commonly used password and validated them to get original password.
2. **URL Interpretation** It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.
3. **File Inclusion attacks** It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.
4. **Man in the middle attacks** It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

**System-based attacks**

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows

1. **Virus** It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.
2. **Worm** It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.
3. **Trojan horse** It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.
4. **Backdoors** It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.
5. **Bots** A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

The 7 layers of cyber security should centre on the mission critical assets you are seeking to protect.

1: Mission Critical Assets – This is the data you need to protect

2: Data Security – Data security controls protect the storage and transfer of data

3: Application Security – Applications security controls protect access to an application, an application’s access to your mission critical assets, and the internal security of the application.

4: Endpoint Security – Endpoint security controls protect the connection between devices and the network.

5: Network Security – Network security controls protect an organization’s network and prevent unauthorized access of the network.

6: Perimeter Security – Perimeter security controls include both the physical and digital security methodologies that protect the business overall.

7: The Human Layer – Humans are the weakest link in any cyber security posture. Human security controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

**Vulnerability, threat, Harmful acts**

As the recent epidemic of data breaches illustrates, no system is immune to attacks. Any company that manages, transmits, stores, or otherwise handles data has to institute and enforce mechanisms to monitor their cyber environment, identify vulnerabilities, and close up security holes as quickly as possible. Before identifying specific dangers to modern data systems, it is crucial to understand the distinction between cyber threats and vulnerabilities.

**Cyber threats** are security incidents or circumstances with the potential to have a negative outcome for your network or other data management systems.

Examples of common types of security threats include phishing attacks that result in the installation of malware that infects your data, failure of a staff member to follow data protection protocols that cause a data breach, or even a tornado that takes down your company’s data headquarters, disrupting access.

**Vulnerabilities** are the gaps or weaknesses in a system that make threats possible and tempt threat actors to exploit them.

Types of vulnerabilities in network security include but are not limited to SQL injections, server misconfigurations, cross-site scripting, and transmitting sensitive data in a nonencrypted plain text format.

When threat probability is multiplied by the potential loss that may result, cyber security experts, refer to this as a risk.

**SECURITY VULNERABILITIES, THREATS AND ATTACKS –**

Categories of vulnerabilities

1. Corrupted (Loss of integrity)
2. Leaky (Loss of confidentiality)
3. Unavailable or very slow (Loss of availability)

Threats represent potential security harm to an asset when vulnerabilities are exploited.

Attacks are threats that have been carried out.

1. **Passive** – Make use of information from the system without affecting system resources.
2. **Active** – Alter system resources or affect operation
3. **Insider** – Initiated by an entity inside the organization
4. **Outsider** – Initiated from outside the perimeter

**Computer criminals**

Computer criminals have access to enormous amounts of hardware, software, and data; they have the potential to cripple much of effective business and government throughout the world. In a sense, the purpose of computer security is to prevent these criminals from doing damage.

We say computer crime is any crime involving a computer or aided by the use of one. Although this definition is admittedly broad, it allows us to consider ways to protect ourselves, our businesses, and our communities against those who use computers maliciously.

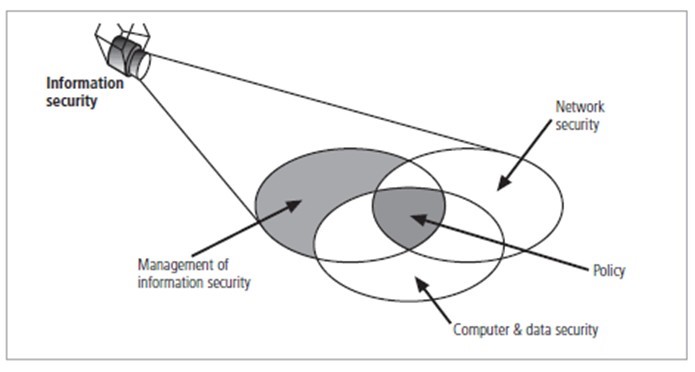
One approach to prevention or moderation is to understand who commits these crimes and why. Many studies have attempted to determine the characteristics of computer criminals. By studying those who have already used computers to commit crimes, we may be able in the future to spot likely criminals and prevent the crimes from occurring.

**What is the CNSS security model?**

CNSS (Committee on National Security Systems is a three-dimensional security model which has now become a standard security model for many of the currently operating information systems. The CNSS model has three key goals of security: Confidentiality, Integrity, and Availability. This comprises one dimension.

**The Committee on National Security Systems (CNSS)**

CNSS defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information [4]. The CNSS Model of information security evolved from a concept developed by the computer security industry called the C.I.A triangle. Figure shows that information security includes broad areas of information security management, computer and data security, and network security.



**CIA Triad**

The CIA Triad is actually a security model that has been developed to help people think about various parts of IT security.

**CIA triad broken down:**

**Confidentiality**

It's crucial in today's world for people to protect their sensitive, private information from unauthorized access.

Protecting confidentiality is dependent on being able to define and enforce certain access levels for information.

In some cases, doing this involves separating information into various collections that are organized by who needs access to the information and how sensitive that information actually is - i.e. the amount of damage suffered if the confidentiality was breached.

Some of the most common means used to manage confidentiality include access control lists, volume and file encryption, and Unix file permissions.

**Integrity**

Data integrity is what the "I" in CIA Triad stands for

This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

**Availability**

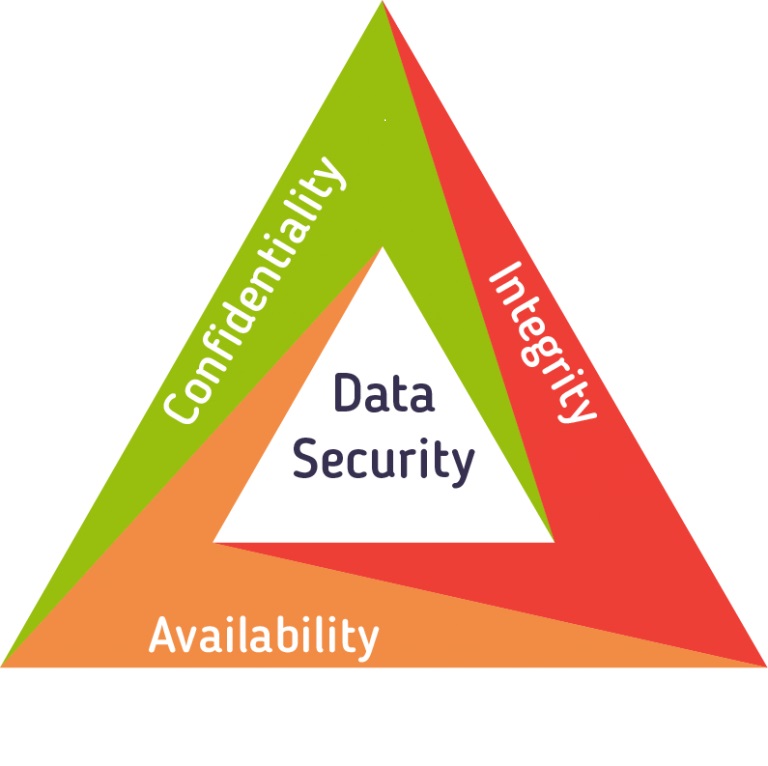
This is the final component of the CIA Triad and refers to the actual availability of your data. Authentication mechanisms, access channels and systems all have to work properly for the information they protect and ensure it's available when it is needed.

Understanding the CIA triad

The CIA Triad is all about information. While this is considered the core factor of the majority of IT security, it promotes a limited view of the security that ignores other important factors.

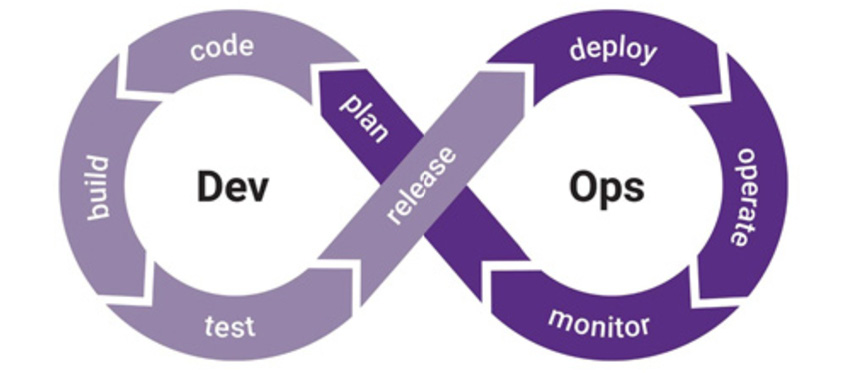
For example, even though availability may serve to make sure you don't lose access to resources needed to provide information when it is needed, thinking about information security in itself doesn't guarantee that someone else hasn't used your hardware resources without authorization.

It's important to understand what the CIA Triad is, how it is used to plan and also to implement a quality security policy while understanding the various principles behind it. It's also important to understand the limitations it presents. When you are informed, you can utilize the CIA Triad for what it has to offer and avoid the consequences that may come along by not understanding it.



## What is the secure SDLC and why should I care?

A software development life cycle (SDLC) is a framework for the process of building an application from inception to decommission. Over the years, [multiple SDLC models](https://www.synopsys.com/blogs/software-security/top-4-software-development-methodologies/) have emerged—from waterfall and iterative to, more recently, [agile](https://www.synopsys.com/glossary/what-is-agile-sdlc.html) and CI/CD, which increase the speed and frequency of deployment.



## In general, SDLCs include the following phases:

* Planning and requirements
* Architecture and design
* Test planning
* Coding
* Testing and results
* Release and maintenance
* In the past, organizations usually performed security-related activities only as part of testing—at the end of the [SDLC](https://www.synopsys.com/glossary/what-is-sdlc.html). As a result of this late-in-the-game technique, they wouldn’t find bugs, flaws, and other vulnerabilities until they were far more expensive and time-consuming to fix. Worse yet, they wouldn’t find any security vulnerabilities at all.
* The [Systems Sciences Institute at IBM](https://www.researchgate.net/figure/255965523_fig1_Figure-3-IBM-System-Science-Institute-Relative-Cost-of-Fixing-Defects) reported that it cost six times more to fix a bug found during implementation than one identified during design. Furthermore, according to IBM, the cost to fix bugs found during the testing phase could be 15 times more than the cost of fixing those found during design.

So it’s far better, not to mention faster and cheaper, to integrate [security testing](https://www.synopsys.com/software-integrity/security-testing.html) across the SDLC, not just at the end, to help discover and reduce vulnerabilities early, effectively building security in. Security assurance activities include [architecture analysis](https://www.synopsys.com/software-integrity/software-security-services/software-architecture-design.html) during design, [code review](https://www.synopsys.com/software-integrity/security-testing/static-analysis-sast.html) during coding and build, and [penetration testing](https://www.synopsys.com/software-integrity/security-testing/penetration-testing.html) before release. Here are some of the primary advantages of a secure SDLC approach:

* Your software is more secure, as security is a continuous concern.
* All stakeholders are aware of security considerations.
* You detect design flaws early, before they’re coded into existence.
* You reduce your costs, thanks to early detection and resolution of defects.
* You reduce overall intrinsic business risks for your organization.

## How does a secure SDLC work?

Generally speaking, a secure SDLC involves integrating [security testing](https://www.synopsys.com/software-integrity.html) and other activities into an existing development process. Examples include writing [security requirements](https://www.synopsys.com/blogs/software-security/software-security-requirements/) alongside functional requirements and performing an [architecture risk analysis](https://www.synopsys.com/software-integrity/software-security-services/software-architecture-design/risk-analysis.html) during the design phase of the SDLC.

Many secure SDLC models are in use, but one of the best known is the [Microsoft Security Development Lifecycle (MS SDL)](https://www.microsoft.com/en-us/securityengineering/sdl/), which outlines 12 practices organizations can adopt to increase the security of their software. And earlier this year, NIST published the final version of its [Secure Software Development Framework](https://doi.org/10.6028/NIST.CSWP.04232020), which focuses on security-related processes that organizations can integrate into their existing SDLC.

**Information Security as an Art**

• Analyze threats to information assets and their risk

• Employ countermeasures to reduce risks, e.g.,

* Harden your OS, shutting down unneeded services.
* Strengthen your network perimeter with firewalls.
* Require strong passwords and strong authentication.

• Such practices are good and useful. But after your system is strong and hard ... what can you actually say about its security?

**Information Security as a Science**

**Science:** the discovery and knowing of something which can be demonstrated and verified within a community.

Example: modern cryptography. **Precise formalism for**

1. **defining what security is** and

2. **making verifiable statements that** (possible under well-defined assumptions) algorithms are secure. Cryptography is very rarely the weak link in application security.