**Information Security & Cyber Security**

* **Cybersecurity**

The activity can be defined as the defending of computers, servers, mobile devices, electronic systems, networks and data from malicious attacks which range from business organizations to personal devices. The attacks are divided into different categories such as network security, application security, information security, operational security, and disaster recovery along with business continuity.

### ****Information security****

Information security in a simplified manner can be described as the prevention of unauthorized access or alteration during the time of storing data or transferring it from one machine to another. The information can be biometrics, social media profile, data on mobile phones etc. due to which, the research for information security covers various sectors such as cryptocurrency and online forensics.

Information security is created to cover three objectives of confidentiality, integrity and availability or as commonly known as CIA.

### ****Differences****

Cybersecurity is meant to protect attacks in cyberspace such as data, storage sources, devices, etc. In contrast, information security is intended to protect data from any form of threat regardless of being analogue or digital. Cybersecurity usually deals with cybercrimes, cyber frauds and law enforcement. On the contrary, information security deals with unauthorized access, disclosure modification and disruption.

Cybersecurity is handled by professionals who are trained to deal with advanced persistent threats (APT) specifically. Information security, on the other hand, lays the foundation of data security and are trained to priorities resources first before eradicating the threats or attacks.

**Information Assurance**

Information assurance (IA) is the practice of protecting against and [managing risk](https://searchcompliance.techtarget.com/definition/risk-management) related to the use, [storage](https://searchstorage.techtarget.com/definition/storage) and transmission of data and information systems. Information assurance processes typically ensure the following functions for [data](https://searchdatamanagement.techtarget.com/definition/data) and associated [information](https://searchsqlserver.techtarget.com/definition/information) systems:

[**Availability**](https://www.techtarget.com/searchnetworking/definition/availability) ensures information is ready for use by those that are allowed to access it and at a required level of performance.

[**Integrity**](https://searchdatacenter.techtarget.com/definition/integrity) ensures that information and associated systems can only be accessed or modified by those authorized to do so.

[**Authentication**](https://www.techtarget.com/searchsecurity/definition/authentication) ensures that users are who they say they are using methods such as individual user names, [passwords](https://www.techtarget.com/searchsecurity/definition/password), [biometrics](https://www.techtarget.com/searchsecurity/definition/biometrics), [digital certificates](https://www.techtarget.com/searchsecurity/definition/digital-certificate) and [security tokens](https://www.techtarget.com/searchsecurity/definition/security-token).

[**Confidentiality**](https://whatis.techtarget.com/definition/confidentiality) limits access or places restrictions on information such as PII or classified corporate data.

[**Non-repudiation**](https://www.techtarget.com/searchsecurity/definition/nonrepudiation) ensures that someone cannot deny an action, such as the receipt of a message or the authenticity of a statement or contract, because the system provides proof of the action.

**Domains of Info-Sec**

The 3 domains of information security are the following:

* Security and Risk Management
* Asset Security
* Security Engineering

So it helps to protect from the following:

* Unauthorized access
* Use
* Exposure
* Division
* Fixing
* Ruin

## **Security and Risk Management**

So security and risk management involve a general understanding.

Also, analysis and risk-mitigating techniques. To determine the team achieves their goal of learning security goals.

So the risk is a major basic in every viewpoint. It is just like information security decisions.

Also, risk management concepts are helping aid each decision. To make effective.

This is the list of the major part of security and risk management.

* Information security within the team
* The triad of information security – Confidentiality, Integrity, and Availability
* Security governance policies
* Business continuity requirements
* Threat modeling
* Policies, standards, procedure, and guidelines
* The idea of risk management

## **Asset Security**

Asset security is focusing on how to controls the custody, labels. The ownership of data and also the data classification clearance.

Data remains is discussing and including recently material.

Also, remain to properties of solid-state drives are combine with ROM and RAM.

It has quite different remaining properties compared to a magnetic drive.

So the asset security binds up with a discussion of control determination. Also adding the scoping and tailoring.

This is the domain address of the material requirements. Cover of the following:

* The classification and ownership of information and assets
* Privacy
* Reservation periods
* Data security controls
* Handling requirements

## **Security Engineering**

Security engineering is representing large and various technical domains.

This domain contains the following:

* Controls used to enforce various levels of confidentiality, availability, integrity
* Secure operating systems and Networks
* The following principles, structures, also concepts
* The implementation and standards used to design
* The application, equipment, and monitoring

So, information security [planning](https://seersco.com/articles/tag/3-domains-of-information-technology/)and design. It covers the practice of applying a wide and accurate method.

It describes a modern or future structure and behavior for a company.

* Organization’s security processes
* Information security systems
* Personnel and organizational sub-units

So security engineering covers several important information security concepts.

* Engineering methods using secure form principles
* Basic ideas of security models
* Security skills of information systems
* Assessing and decreasing vulnerabilities in systems
* Cryptography
* Designing and achieving physical security

So that is the three-domain of information security. It is very helpful for our security in our daily lives.

So this domain is protecting our data of confidentiality, integrity, and availability. From the cybercrimes.