


Information Security Overview

Information security refers to the protection or safeguarding of information and information systems that use, store, and transmit information from unauthorized access, disclosure, alteration, and destruction. Information is a critical asset that organizations must secure. If sensitive information falls into the wrong hands, then the respective organization may suffer huge losses in terms of finances, brand reputation, customers, or in other ways. To provide an understanding of how to secure such critical information resources, this module starts with an overview of information security.

This section introduces the elements of information security, classification of attacks, and information warfare.

Elements of Information Security



Information security is a state of well-being of information and infrastructure in which the possibility of **theft, tampering,** and **disruption of information and services** is low or tolerable

Confidentiality	Assurance that the information is accessible only to those authorized to have access
Integrity	The trustworthiness of data or resources in terms of preventing improper or unauthorized changes
Availability	Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users
Authenticity	Refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine
Non-Repudiation	A guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Elements of Information Security

Information security is “the state of the well-being of information and infrastructure in which the possibility of theft, tampering, or disruption of information and services is kept low or tolerable.” It relies on five major elements: confidentiality, integrity, availability, authenticity, and non-repudiation.

- **Confidentiality**

Confidentiality is the assurance that the information is accessible only to authorized. Confidentiality breaches may occur due to improper data handling or a hacking attempt. Confidentiality controls include data classification, data encryption, and proper disposal of equipment (such as DVDs, USB drives, and Blu-ray discs).

- **Integrity**

Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes—the assurance that information is sufficiently accurate for its purpose. Measures to maintain data integrity may include a checksum (a number produced by a mathematical function to verify that a given block of data is not changed) and access control (which ensures that only authorized people can update, add, or delete data).

- **Availability**

Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users. Measures to maintain data availability can include disk arrays for redundant systems and clustered machines, antivirus software to combat malware, and distributed denial-of-service (DDoS) prevention systems.

- **Authenticity**

Authenticity refers to the characteristic of communication, documents, or any data that ensures the quality of being genuine or uncorrupted. The major role of authentication is to confirm that a user is genuine. Controls such as biometrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, and documents.

- **Non-Repudiation**

Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Individuals and organizations use digital signatures to ensure non-repudiation.