

# Ethical Hacking Essential (EHE)

Prepared By Dr. Kamal Alieyan

## Lecture 01



## Module 01

# Information Security Fundamentals



# Module Objectives

- 1 Understanding the Need for Security
- 2 Understanding the Elements of Information Security
- 3 Understanding the Security, Functionality, and Usability Triangle
- 4 Understanding Motives, Goals, and Objectives of Information Security Attacks
- 5 Overview of Classification of Attacks
- 6 Overview of Information Security Attack Vectors
- 7 Overview of Various Information Security Laws and Regulations

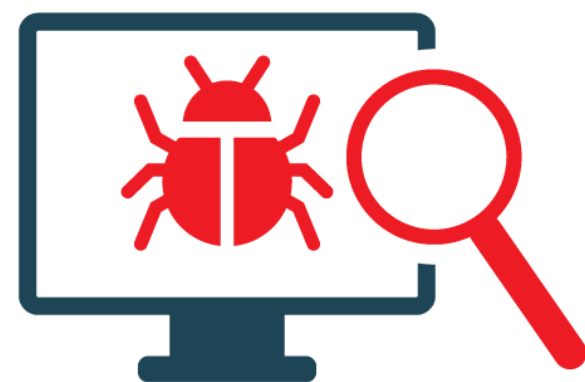
# Module Flow

1

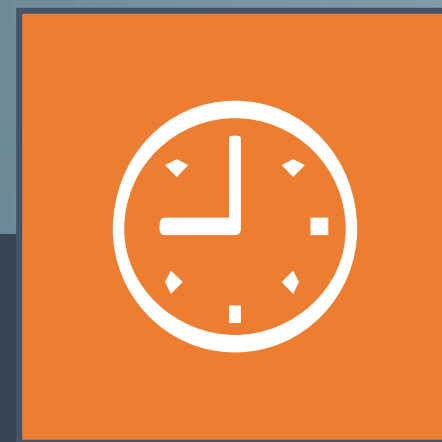
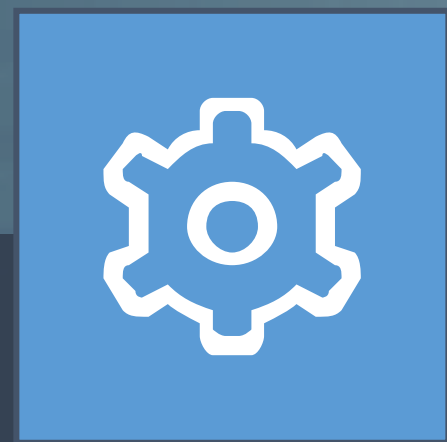
**Discuss Information Security Fundamentals**

2

**Discuss Various Information Security Laws and Regulations**



# What is Information Security?



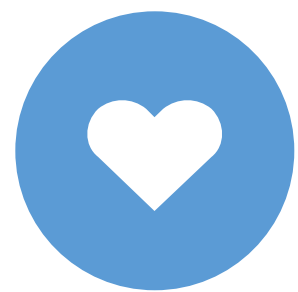
Information security is a state of well-being of information and infrastructure in which the possibility of **theft, tampering, and disruption of information and services is low or tolerable**

# Need for Security

- Evolution of technology, focused on **ease of use** 01
- Rely on the use of computers for accessing, providing, or just storing information 02
- Increased **network environment** and network-based applications 03
- Direct impact of **security breach** on the corporate asset base and goodwill 04
- Increasing complexity** of computer infrastructure administration and management 05



# Elements of Information Security



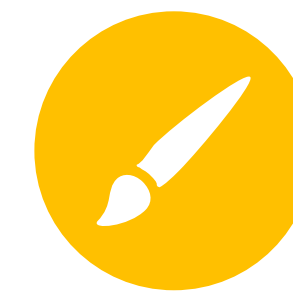
## Confidentiality

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



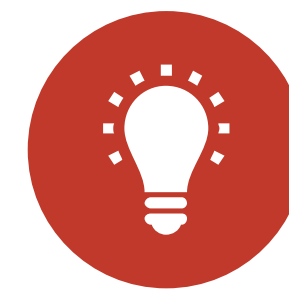
## Availability

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

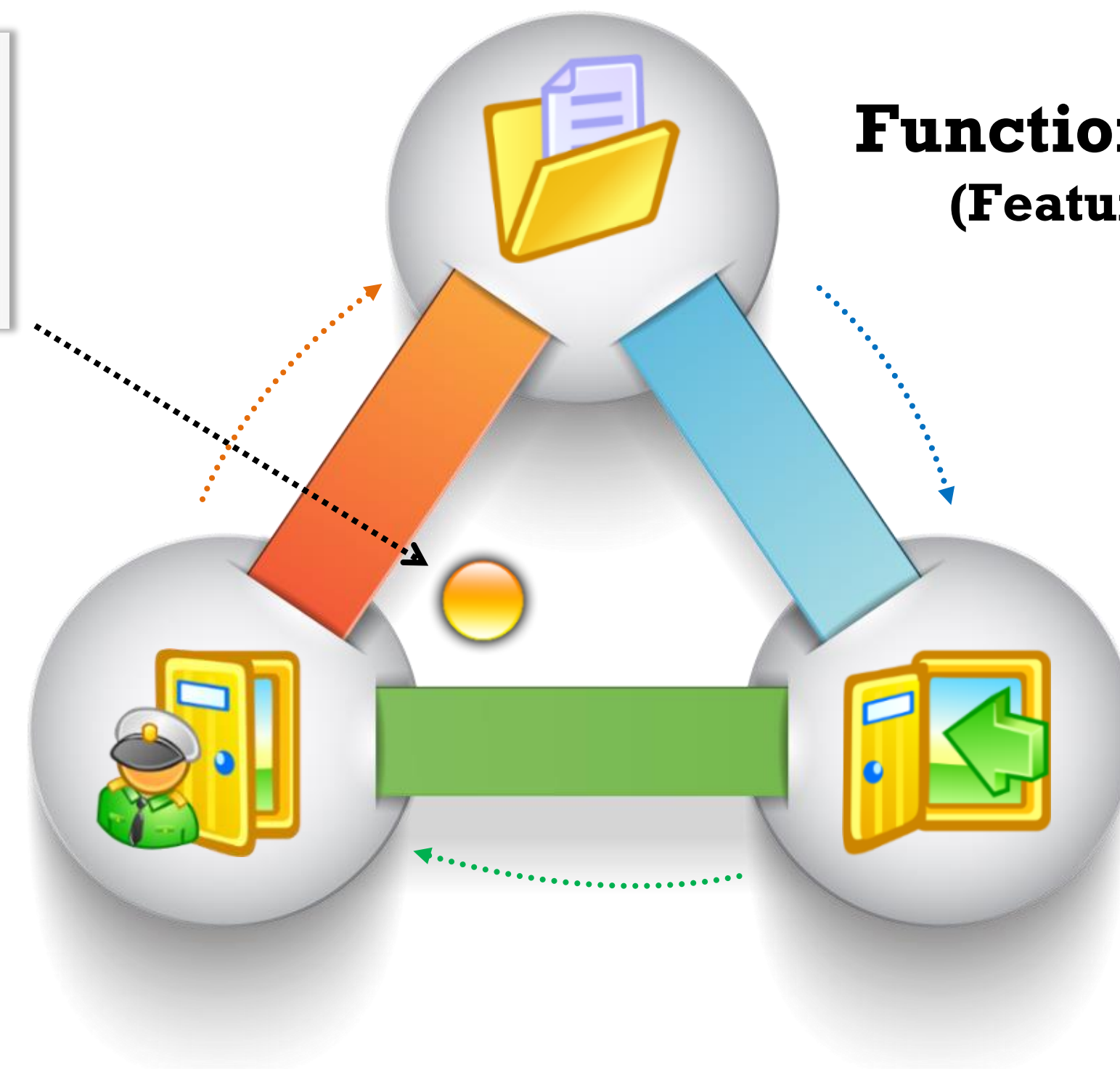
# The Security, Functionality, and Usability Triangle



**Level of security** in any system can be defined by the strength of three components:

Moving the ball towards security means less functionality and usability

**Security**  
(Restrictions)



**Functionality**  
(Features)

**Usability**  
(GUI)

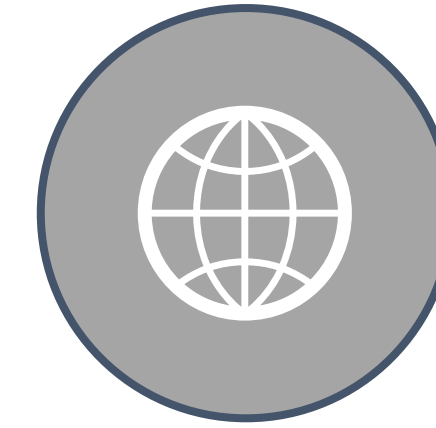
# Security Challenges



**Compliance** to government laws and regulations



Lack of **qualified and skilled** cybersecurity professionals



Difficulty in centralizing security in a **distributed computing environment**



**Fragmented** and **complex** privacy and data protection regulations



Compliance issues due to the implementation of **Bring Your Own Device** (BYOD) policies in companies



Relocation of sensitive data from **legacy data centers** to the cloud without proper configuration

# Motives, Goals, and Objectives of Information Security Attacks

**Attacks** = Motive (Goal) + Method + Vulnerability



A motive originates out of the notion that the **target system stores or processes** something valuable, and this leads to the threat of an attack on the system



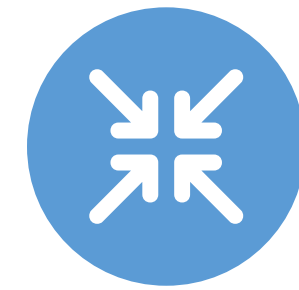
Attackers try various tools and attack techniques to **exploit vulnerabilities** in a computer system or its security policy and controls in order to fulfil their motives



## Motives behind information security attacks

- ✓ Disrupting business continuity
- ✓ Stealing information and manipulating data
- ✓ Creating fear and chaos by disrupting critical infrastructures
- ✓ Causing financial loss to the target
- ✓ Damaging the reputation of the target

# Classification of Attacks



## Passive Attacks

- Do not tamper with the data and involve intercepting and **monitoring network traffic** and data flow on the target network
- Examples include sniffing and eavesdropping



## Active Attacks

- Tamper with the data in transit or **disrupt the communication** or services between the systems to bypass or break into secured systems
- Examples include DoS, Man-in-the-Middle, session hijacking, and SQL injection



## Close-in Attacks

- Are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or **disrupt access** to information
- Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving

# Classification of Attacks (Cont'd)



## Insider Attacks

- Involve using privileged access to **violate rules** or intentionally cause a threat to the organization's information or information systems
- Examples include theft of physical devices and planting keyloggers, backdoors, and malware



## Distribution Attacks

- Occur when attackers **tamper with hardware** or **software** prior to installation
- Attackers tamper with the hardware or software at its source or in transit

# Information Security Attack Vectors



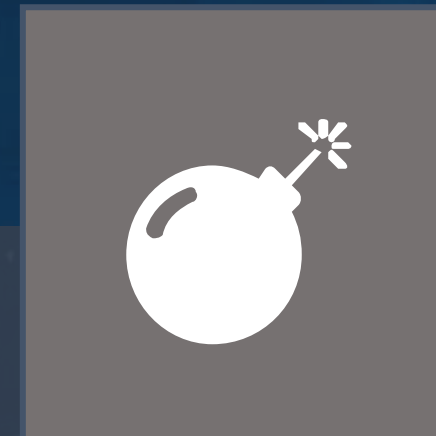
## Cloud Computing Threats

Cloud computing is an **on-demand delivery of IT capabilities** where sensitive data of organizations, and their clients is stored. Flaw in one client's application cloud allow attackers to access other client's data



## Advanced Persistent Threats (APT)

An attack that is focused on **stealing information from the victim machine** without the user being aware of it



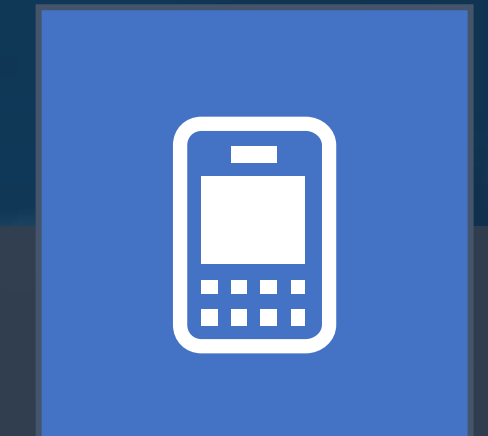
## Viruses and Worms

The most prevalent networking threat that are **capable of infecting a network within seconds**



## Ransomware

**Restricts access** to the computer system's files and folders and **demands an online ransom payment** to the malware creator(s) in order to remove the restrictions



## Mobile Threats

Focus of attackers has shifted to **mobile devices** due to increased adoption of mobile devices for business and personal purposes and comparatively **lesser security controls**

# Information Security Attack Vectors (Cont'd)

## Botnet

A huge **network of the compromised systems** used by an intruder to perform various network attacks



## Insider Attack

An **attack performed on a corporate network** or on a single computer by an **entrusted person (insider)** who has authorized access to the network

## Phishing

The practice of **sending an illegitimate email** falsely claiming to be from a **legitimate site** in an attempt to **acquire a user's personal or account information**

## Web Application Threats

Attackers target web applications to steal credentials, set up phishing site, or **acquire private information** to threaten the performance of the website and hamper its security

## IoT Threats

- IoT devices include many software applications that are used to **access the device remotely**
- Flaws in the IoT devices allows attackers access into the device remotely and perform various attacks

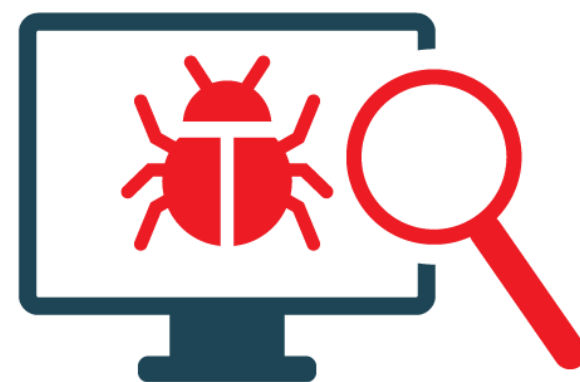
# Module Flow

1

**Discuss Information Security Fundamentals**

2

**Discuss Various Information Security Laws and Regulations**



# Payment Card Industry Data Security Standard (PCI DSS)



- ❑ A proprietary **information security standard for organizations** that handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards
- ❑ PCI DSS **applies to all entities involved in payment card processing** — including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data

## PCI Data Security Standard — High Level Overview



Build and Maintain a Secure Network



Protect Cardholder Data



Maintain a Vulnerability Management Program



Implement Strong Access Control Measures



Regularly Monitor and Test Networks



Maintain an Information Security Policy

<https://www.pcisecuritystandards.org>

Failure to meet the PCI DSS requirements may result in fines or the termination of payment card processing privileges

# ISO/IEC 27001:2013

- ❑ Specifies the requirements for **establishing, implementing, maintaining**, and continually improving an **information security management system** within the context of the organization
- ❑ It is intended to be suitable for several different types of use, including:

Use within organizations to formulate **security requirements** and **objectives**



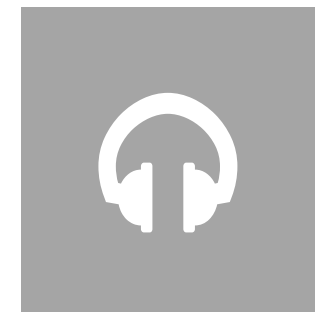
Identification and clarification of existing **information security management processes**

Use within organizations to ensure that security risks are **cost-effectively managed**



Use by organization management to determine the **status of information security management activities**

Use within organizations to **ensure compliance with laws and regulations**



Implementation of **business-enabling information security**

Definition of new **information security management processes**



Use by organizations to provide relevant information about **information security** to customers

# Health Insurance Portability and Accountability Act (HIPAA)

HIPPA  
SECURITY

Electronic  
Transaction and  
Code Set Standards



Requires every provider who does business electronically to **use the same health care transactions, code sets, and identifiers**

Privacy Rule



Provides **federal protections for the personal health information** held by covered entities and gives patients an array of rights with respect to that information

Security Rule



Specifies a series of administrative, physical, and technical safeguards for covered entities to use to ensure the **confidentiality, integrity, and availability of electronically protected health information**

National Identifier  
Requirements



Requires that health care providers, health plans, and employers have standard national numbers that identify them attached to **standard transactions**

Enforcement Rule



Provides the standards for enforcing all the **Administration Simplification Rules**

## HIPAA's Administrative Simplification Statute and Rules

<https://www.hhs.gov>

# Sarbanes Oxley Act (SOX)

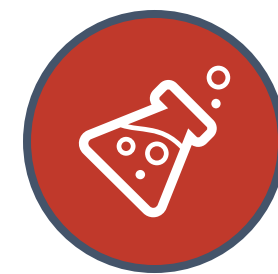


- ❑ Enacted in 2002, the Sarbanes-Oxley Act is designed to **protect investors and the public** by increasing the accuracy and reliability of corporate disclosures
- ❑ The key requirements and provisions of SOX are organized into **11 titles**:



## **Title I**

**Public Company Accounting Oversight Board (PCAOB)**  
provides independent oversight of public accounting firms providing audit services (“auditors”)



## **Title II**

**Auditor Independence** establishes the standards for external auditor independence, intended to limit conflicts of interest and address new auditor approval requirements, audit partner rotation, and auditor reporting requirements



## **Title III**

**Corporate Responsibility**  
mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports

<https://www.sec.gov>

# Sarbanes Oxley Act (SOX) (Cont'd)



## Title IV

**Enhanced Financial Disclosures** describe enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and the stock transactions of corporate officers



## Title V

**Analyst Conflicts of Interest** consist of measures designed to help restore investor confidence in the reporting of securities analysts



## Title VI

**Commission Resources and Authority** defines practices to restore investor confidence in securities analysts



## Title VII

**Studies and Reports** includes the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing, or others to manipulate earnings and obfuscate true financial conditions

# Sarbanes Oxley Act (SOX) (Cont'd)



## **Title VIII**

**Corporate and Criminal Fraud Accountability** describes specific criminal penalties for fraud by the manipulation, destruction, or alteration of financial records, or other interference with investigations while providing certain protections for whistle-blowers



## **Title X**

**White Collar Crime Penalty Enhancement** increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds the failure to certify corporate financial reports as a criminal offense



## **Title IX**

**Corporate Tax Returns** states that the Chief Executive Officer should sign the company tax return



## **Title XI**

**Corporate Fraud Accountability** identifies corporate fraud and record tampering as criminal offenses and assigns them specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to temporarily freeze large or unusual payments



# The Digital Millennium Copyright Act (DMCA)



- ❑ The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization** (WIPO)
- ❑ It **defines the legal prohibitions** against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information

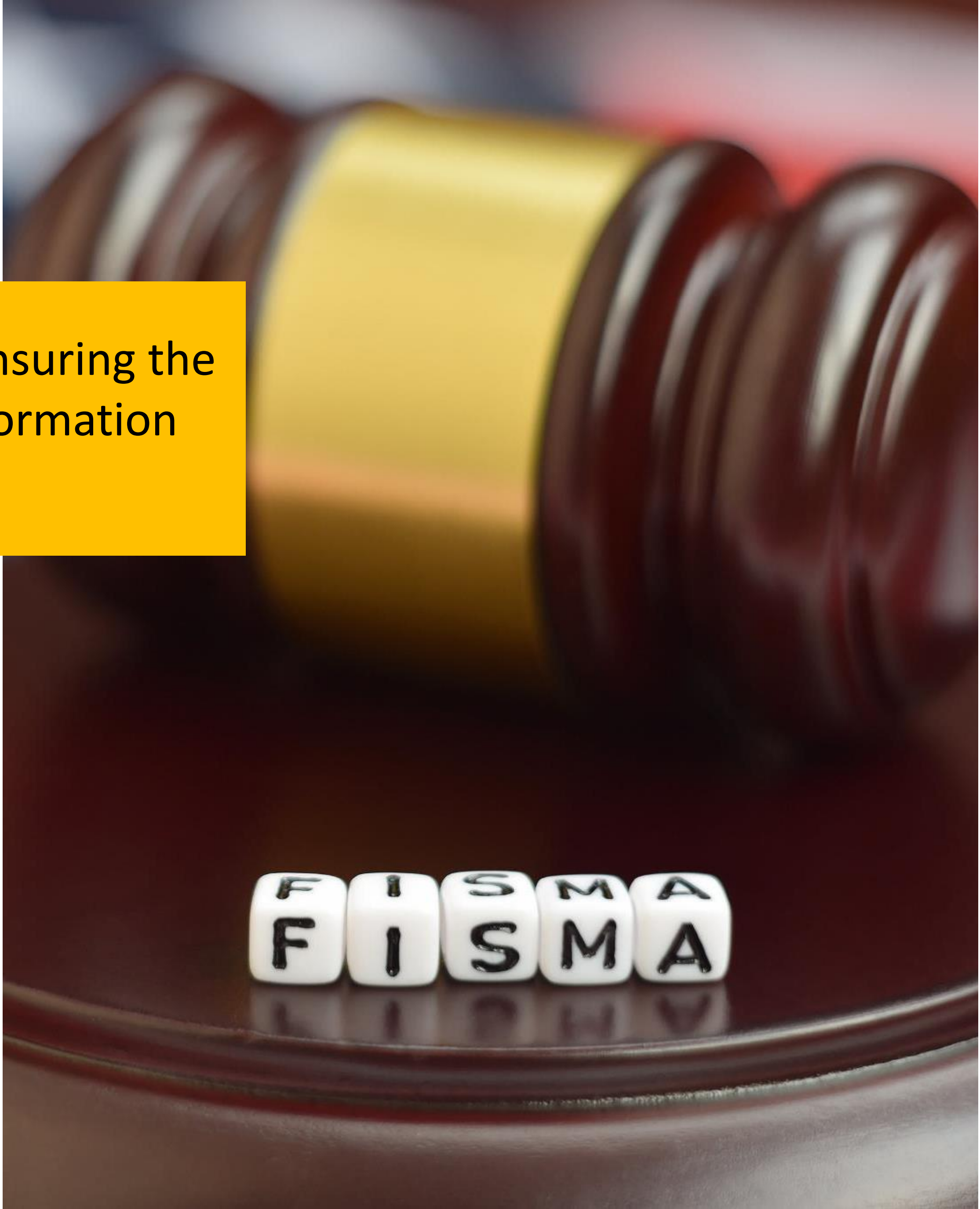
# The Federal Information Security Management Act (FISMA)

The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support Federal operations and assets

It includes

- Standards for categorizing information and information systems by mission impact
- Standards for minimum security requirements for information and information systems
- Guidance for selecting appropriate security controls for information systems
- Guidance for assessing security controls in information systems and determining security control effectiveness
- Guidance for security authorization of information systems

<https://csrc.nist.gov>

A close-up photograph of a combination lock with several tumblers. The tumblers are arranged to spell out the acronym 'FISMA' in white letters on a dark, polished metal surface. The background is blurred, showing more of the lock mechanism.

FISMA



- ❑ GDPR regulation was put into effect on May 25, 2018 and one of the **most stringent privacy and security laws globally**
- ❑ The GDPR will **levy harsh fines** against those who violate its privacy and security standards, with penalties reaching tens of millions of euros

### GDPR Data Protection Principles

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

## General Data Protection Regulation (GDPR)

<https://gdpr.eu>

# Data Protection Act 2018 (DPA)

The DPA is an act to make provision for the regulation of the processing of information relating to **individuals**; to make provision in connection with the **Information Commissioner's functions** under specific regulations relating to information; to make provision for a direct **marketing code** of practice, and connected purposes

The DPA **protects individuals** concerning the processing of personal data, in particular by:

- Requiring **personal data to be processed lawfully** and fairly, based on the data subject's consent or another specified basis,
- **Conferring rights** on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, and
- **Conferring functions** on the Commissioner, giving the holder of that office responsibility to monitor and enforce their provisions

<https://www.legislation.gov.uk>

# Cyber Law in Different Countries

| Country Name  | Laws/Acts                                                            | Website                                                             |
|---------------|----------------------------------------------------------------------|---------------------------------------------------------------------|
| United States | Section 107 of the Copyright Law mentions the doctrine of “fair use” | <a href="https://www.copyright.gov">https://www.copyright.gov</a>   |
|               | Online Copyright Infringement Liability Limitation Act               |                                                                     |
|               | The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)                   | <a href="https://www.uspto.gov">https://www.uspto.gov</a>           |
|               | The Electronic Communications Privacy Act                            | <a href="https://fas.org">https://fas.org</a>                       |
|               | Foreign Intelligence Surveillance Act                                | <a href="https://fas.org">https://fas.org</a>                       |
|               | Protect America Act of 2007                                          | <a href="https://www.justice.gov">https://www.justice.gov</a>       |
|               | Privacy Act of 1974                                                  | <a href="https://www.justice.gov">https://www.justice.gov</a>       |
|               | National Information Infrastructure Protection Act of 1996           | <a href="https://www.nrotc.navy.mil">https://www.nrotc.navy.mil</a> |
|               | Computer Security Act of 1987                                        | <a href="https://csrc.nist.gov">https://csrc.nist.gov</a>           |
|               | Freedom of Information Act (FOIA)                                    | <a href="https://www.foia.gov">https://www.foia.gov</a>             |
|               | Computer Fraud and Abuse Act                                         | <a href="https://energy.gov">https://energy.gov</a>                 |
|               | Federal Identity Theft and Assumption Deterrence Act                 | <a href="https://www.ftc.gov">https://www.ftc.gov</a>               |

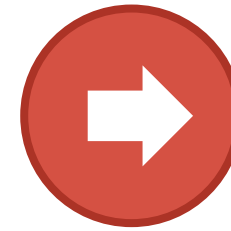
# Cyber Law in Different Countries (Cont'd)

| Country Name   | Laws/Acts                                                                                       | Website                                                                     |
|----------------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Australia      | The Trade Marks Act 1995                                                                        | <a href="https://www.legislation.gov.au">https://www.legislation.gov.au</a> |
|                | The Patents Act 1990                                                                            |                                                                             |
|                | The Copyright Act 1968                                                                          |                                                                             |
|                | Cybercrime Act 2001                                                                             |                                                                             |
| United Kingdom | The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002                          | <a href="https://www.legislation.gov.uk">https://www.legislation.gov.uk</a> |
|                | Trademarks Act 1994 (TMA)                                                                       |                                                                             |
|                | Computer Misuse Act 1990                                                                        |                                                                             |
|                | The Network and Information Systems Regulations 2018                                            |                                                                             |
|                | Communications Act 2003                                                                         |                                                                             |
|                | The Privacy and Electronic Communications (EC Directive) Regulations 2003                       |                                                                             |
|                | Investigatory Powers Act 2016                                                                   |                                                                             |
|                | Regulation of Investigatory Powers Act 2000                                                     |                                                                             |
| China          | Copyright Law of the People's Republic of China (Amendments on October 27, 2001)                | <a href="http://www.npc.gov.cn">http://www.npc.gov.cn</a>                   |
|                | Trademark Law of the People's Republic of China (Amendments on October 27, 2001)                |                                                                             |
| India          | The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957               | <a href="http://www.ipindia.nic.in">http://www.ipindia.nic.in</a>           |
|                | Information Technology Act                                                                      | <a href="https://www.meity.gov.in">https://www.meity.gov.in</a>             |
| Germany        | Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage | <a href="https://www.cybercrimelaw.net">https://www.cybercrimelaw.net</a>   |

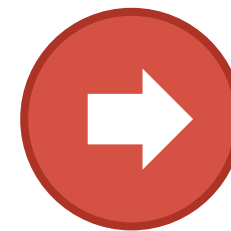
# Cyber Law in Different Countries (Cont'd)

| Country Name | Laws/Acts                                                                                    | Website                                                                       |
|--------------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Italy        | Penal Code Article 615 ter                                                                   | <a href="https://www.cybercrimelaw.net">https://www.cybercrimelaw.net</a>     |
| Japan        | The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000) | <a href="https://www.iip.or.jp">https://www.iip.or.jp</a>                     |
| Canada       | Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1   | <a href="https://laws-lois.justice.gc.ca">https://laws-lois.justice.gc.ca</a> |
| Singapore    | Computer Misuse Act                                                                          | <a href="https://sso.agc.gov.sg">https://sso.agc.gov.sg</a>                   |
| South Africa | Trademarks Act 194 of 1993                                                                   | <a href="http://www.cipc.co.za">http://www.cipc.co.za</a>                     |
|              | Copyright Act of 1978                                                                        | <a href="https://www.nlsa.ac.za">https://www.nlsa.ac.za</a>                   |
| South Korea  | Copyright Law Act No. 3916                                                                   | <a href="https://www.copyright.or.kr">https://www.copyright.or.kr</a>         |
|              | Industrial Design Protection Act                                                             | <a href="https://www.kipo.go.kr">https://www.kipo.go.kr</a>                   |
| Belgium      | Copyright Law, 30/06/1994                                                                    | <a href="https://www.wipo.int">https://www.wipo.int</a>                       |
|              | Computer Hacking                                                                             | <a href="https://www.cybercrimelaw.net">https://www.cybercrimelaw.net</a>     |
| Brazil       | Unauthorized modification or alteration of the information system                            | <a href="https://www.domstol.no">https://www.domstol.no</a>                   |
| Hong Kong    | Article 139 of the Basic Law                                                                 | <a href="https://www.basiclaw.gov.hk">https://www.basiclaw.gov.hk</a>         |

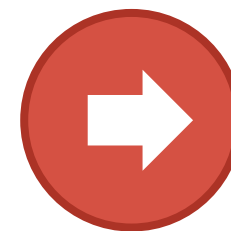
# Module Summary



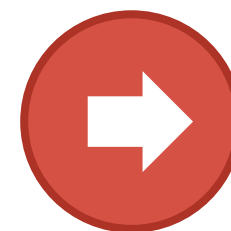
This module has discussed the need for security, elements of information security, the security, functionality, and usability triangle, and security challenges



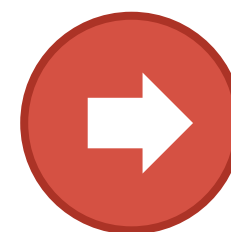
It has covered motives, goals, and objectives of information security attacks in detail



It also discussed classification of attacks and information security attack vectors



Finally, this module ended with a detailed discussion of various information security laws and regulations



The next module will give you introduction on ethical hacking fundamental concepts such as cyber kill chain methodology, hacking concepts, hacker classes, and various phases of hacking cycle