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**

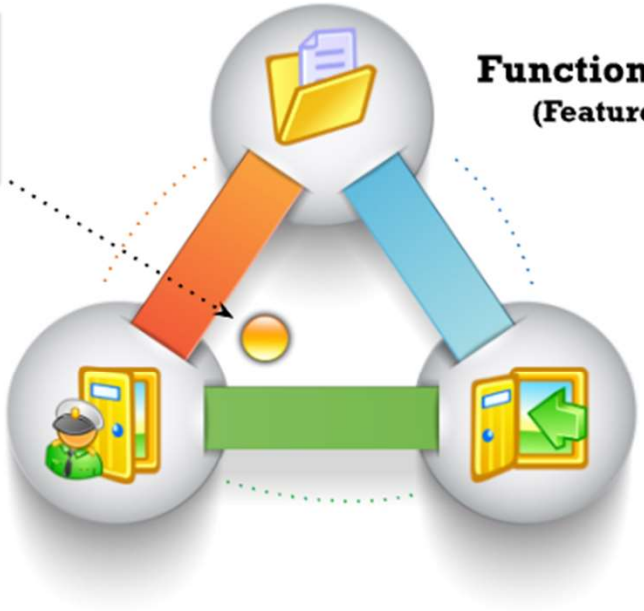
Need for Security

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

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 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

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

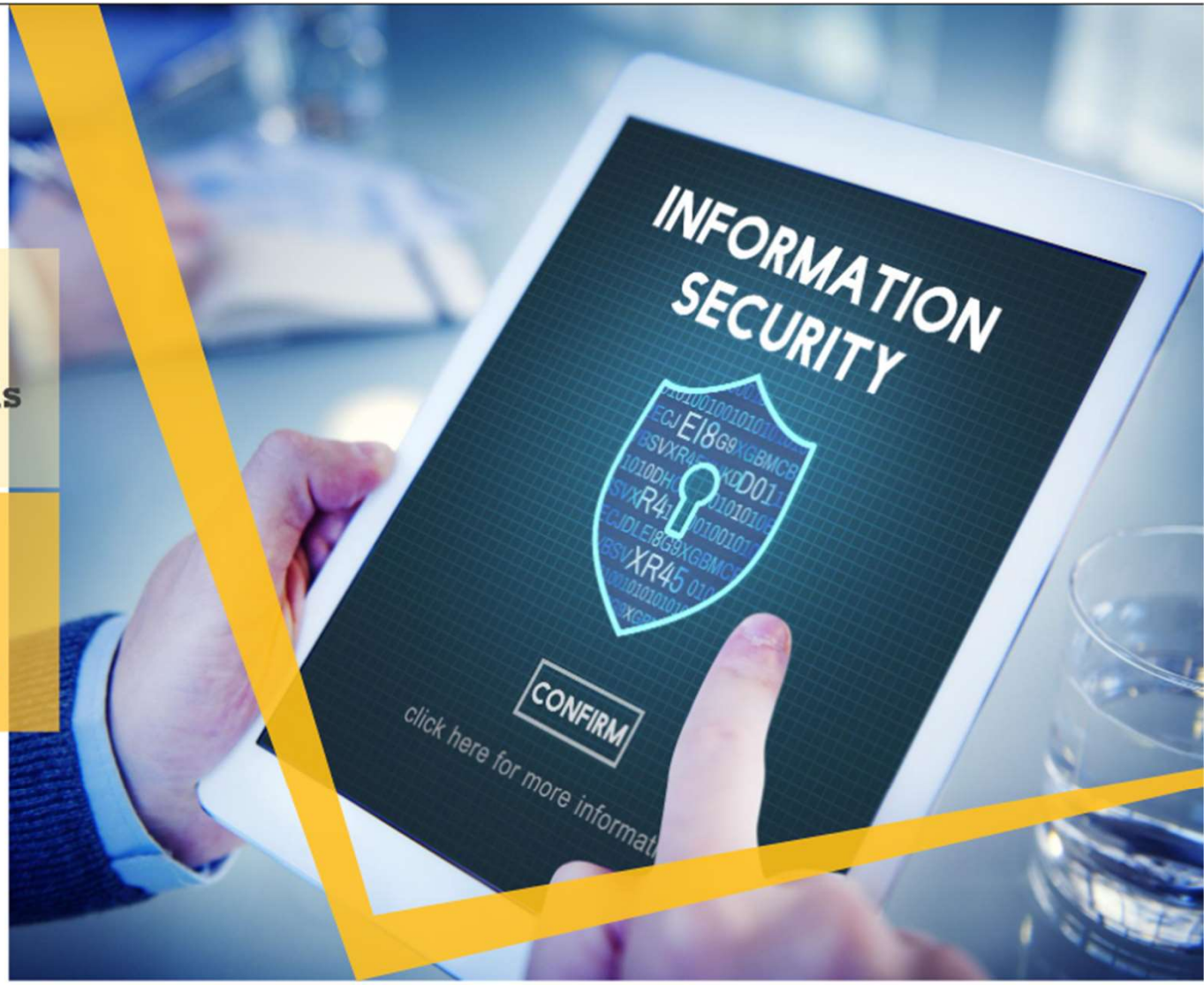
Attackers target web applications to steal credentials, set up phishing site, or **acquire private information** to threaten the performance of the website and hamper its security

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

https://www.iso.org

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA's Administrative Simplification Statute and Rules

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**

https://www.hhs.gov

Cyber Law in Different Countries

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

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	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)	http://www.npc.gov.cn
	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	http://www.ipindia.nic.in
	Information Technology Act	https://www.meity.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net

Cyber Law in Different Countries (Cont'd)

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

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