St. Francis Institute of Technology, Mumbai-400 103
Autonomous Institute
Department Of Information Technology

A.Y. 2024-2025
Class: BE-IT A/B, Semester: VII

Subject: Secure Application Development Lab

Student Name: Durva Kadam Student Roll No: 23

Experiment – 1: Study of different laws and standards of Cyber Security

Aim: To study of different laws and standards of cyber security

Objective: After performing the experiment, the students will be able to –

- To know Cyber security
- Read and understand Different cyber law and standards
- To understand the cyber Security

Lab objective mapped: To **apply** secure programming of application code

Prerequisite: Basic knowledge Information Security

Requirements: Personal Computer, Windows operating system browser, Internet Connection etc.

.

Pre-Experiment Theory:

What is Cyber Security?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.

These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information.

Role of Cyber Laws in Cybersecurity

Cyber laws are integral to the use of the internet and serve a variety of purposes. Most of these laws are there to protect users from becoming victims of cybercrimes, while others are made to regulate the usage of the internet and computers in general. Cyber laws cover these three primary areas:

- **Fraud:** Cyber laws protect users from falling victim to online fraud. They exist to prevent crimes such as credit card and identity theft. These laws also declare federal and state criminal charges for anyone that attempts to commit such fraud.

- **Copyright:** Cyber laws also prevent copyright infringement and enforce copyright protection. They provide individuals and businesses with the right to protect their creative works and to profit from them.
- **Defamation:** Cyber laws are also enforced in online defamation cases, which provide individuals and businesses protection against false allegations made online that can be harmful to their reputations.

Cyber Security Laws in India

India has four predominant laws when it comes to cybersecurity:

- **Information Technology Act (2000):** Enacted by the parliament of India, the information technology act was made to safeguard the e-governance, e banking, and e-commerce sectors.
- **Indian Penal Code (IPC) (1980):** This cybercrime prevention act has primary relevance to cyber frauds concerning identity theft and other sensitive information theft.
- **Companies Act (2013):** With the companies act enacted back in 2013, the legislature ensured that all the regulatory compliances are covered, including e-discovery, cyber forensics, and cybersecurity diligence. The Companies Act provides guidelines for the responsibilities of the company directors and leaders concerning confirming cybersecurity obligations.
- **NIST Compliance:** The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), contains all the guidelines, standards, and best practices necessary to responsibly address cybersecurity risks.

Procedure

- Define Cyber Security

Cybersecurity is the practice of protecting digital systems, networks, and data from threats such as attacks, unauthorized access, and damage. It ensures the confidentiality, integrity, and availability of information.

Types of Cybersecurity

- Network Security: Protects network infrastructure using firewalls, IDS/IPS, and secure design.
- Information Security: Safeguards data confidentiality and integrity with encryption and access controls.
- Application Security: Secures software applications from vulnerabilities through secure coding and testing.
- Endpoint Security: Protects individual devices with antivirus software and management policies.
- Cloud Security: Ensures data protection and secure access in cloud environments.
- Operational Security: Involves incident response and risk management practices.
- Identity and Access Management (IAM): Manages user access through authentication and authorization controls.

Cyber Laws in India

- Information Technology Act, 2000 (IT Act): Governs electronic transactions, cybercrimes, and digital signatures. Includes amendments for data protection and cyber terrorism.
- Personal Data Protection Bill, 2019: Proposed legislation for comprehensive data protection (still under discussion).
- Indian Penal Code (IPC): Includes amendments for cyber-related crimes.
- National Critical Information Infrastructure Protection Centre (NCIIPC): Protects critical infrastructure.
- CERT-In: Provides support and guidance on cyber incidents.

- Discuss different types of Cyber threats. (minimum 5)

Types of Cyber Threats

- **Malware**: This category includes various types of malicious software designed to harm or exploit computers and networks. Common types of malware include viruses, worms, Trojans, ransomware, and spyware. Malware can steal personal information, encrypt files for ransom, or cause general system malfunctions.
- **Phishing**: Phishing attacks involve tricking individuals into divulging sensitive information, such as usernames, passwords, or financial details, by pretending to be a legitimate entity. This is often done through deceptive emails, fake websites, or fraudulent phone calls.
- **Denial of Service (DoS) Attacks**: DoS attacks overwhelm a system or network with excessive traffic, rendering it unavailable to users. This can be executed by a single source (DoS) or multiple sources (Distributed Denial of Service, or DDoS).
- **Man-in-the-Middle (MitM) Attacks**: In these attacks, an adversary intercepts and potentially alters the communication between two parties without their knowledge. This can lead to unauthorized access to sensitive data or manipulation of the communication.
- **SQL Injection**: This attack involves inserting malicious SQL queries into an input field, which can then be executed by the backend database.

- What happens if anyone breaks a cyber-law?

Consequences of Breaking Cyber-Laws

- **Criminal Penalties**: Individuals found guilty of violating cyber laws can face severe criminal penalties, including fines and imprisonment. The severity of the punishment often depends on the nature of the crime and the damage caused.
- **Civil Liabilities**: Offenders may also be subject to civil lawsuits, where they can be required to pay damages to the affected parties. This is especially common in cases of data breaches or unauthorized access.
- **Reputation Damage**: Being caught breaking cyber laws can significantly damage an individual's or organization's reputation, leading to loss of trust.
- **Legal Costs**: Defending against cybercrime charges can be expensive, involving legal fees, settlements, and other associated costs.

- **Employment Consequences**: Individuals convicted of cybercrimes may face difficulties in finding or retaining employment, particularly in the technology and security fields.

- Importance of Cyber Law and standards

Importance of Cyber Law and Standards

- **Protecting Data and Privacy**: Cyber laws and standards are crucial for safeguarding personal and sensitive information from unauthorized access, misuse, or theft. They help ensure that individuals' and organizations' data are handled with care and respect.
- **Maintaining Security**: These laws help to establish security protocols and best practices, which are essential for protecting systems and networks from various cyber threats.
- **Promoting Trust**: Clear and enforced cyber laws foster trust between consumers and organizations. When people know that their data is protected by legal standards, they are more likely to engage with digital services and platforms.
- **Encouraging Compliance**: Regulations and standards set a baseline for cybersecurity practices, ensuring that organizations follow required measures to protect themselves and their customers.
- **Facilitating International Cooperation**: Cyber threats often cross national boundaries, and standardized laws and regulations help countries cooperate in addressing and mitigating these threats.

- What are the areas involved in Cyber Law?
  - **Data Protection and Privacy**: Regulations governing how personal data should be collected, stored, and shared, such as GDPR in Europe or CCPA in California.
  - **Cybercrime**: Laws addressing various types of cybercrime, including hacking, identity theft, and online fraud.
  - **Intellectual Property**: Protection of digital intellectual property rights, including copyrights, trademarks, and patents related to software and digital content.
  - **Electronic Transactions**: Regulations concerning online transactions, digital contracts, and electronic signatures.
  - **Cybersecurity Standards**: Guidelines and frameworks for ensuring the security of information systems and networks.

- What are the standards you study in Cyber Law?

Standards in Cyber Law

- **ISO/IEC 27001**: An international standard for information security management systems (ISMS), providing a systematic approach to managing sensitive company information.

- **NIST Cybersecurity Framework**: A set of guidelines developed by the National Institute of Standards and Technology (NIST) to improve the security of critical infrastructure.
- **General Data Protection Regulation (GDPR)**: A regulation in EU law on data protection and privacy, focusing on how personal data should be handled.
- **Payment Card Industry Data Security Standard (PCI DSS)**: A standard for ensuring that all companies that process, store, or transmit credit card information maintain a secure environment.
- **Health Insurance Portability and Accountability Act (HIPAA)**: A U.S. regulation that provides standards for protecting sensitive patient information.

- How to protect yourself on the Internet?
  - **Use Strong Passwords**: Create complex passwords with a mix of letters, numbers, and symbols. Avoid using the same password for multiple accounts.
  - **Enable Two-Factor Authentication** (2FA): Add an extra layer of security to your accounts by requiring a second form of verification in addition to your password.
  - **Keep Software Updated**: Regularly update your operating system, applications, and antivirus software to protect against known vulnerabilities.
  - **Be Wary of Phishing Scams**: Be cautious about unsolicited emails, messages, or links. Verify the authenticity of the sender before clicking on any links or providing personal information.
  - **Use Secure Connections**: Avoid using public Wi-Fi for sensitive transactions. Use a VPN (Virtual Private Network) to encrypt your internet connection and protect your privacy.
  - **Regularly Backup Data**: Ensure that your important files are backed up regularly to mitigate the effects of data loss or ransomware attacks.

Post-Experiments Exercise

Post Experimental Exercise-
Questions:
Discuss the real world incidence related to cyber threat?

Conclusion:
Explain the importance of cyber security laws and standards based on your learnings from this experiment.

References:

○ **https://www.udemy.com/course/secure-coding-secure-application-development/**
○ **https://kirkpatrickprice.com/blog/secure-coding-best-practices/**