St. Francis Institute of Technology
(An Autonomous Institution)
AICTE Approved | Affiliated to University of Mumbai

A+ Grade by NAAC: CMPN, EXTC, INFT NBA Accredited: ISO 9001:2015 Certified

Department of Information Technology

A.Y. 2025-2026
Class: BE-IT A/B, Semester: VIII
Subject: Secure Application Development Lab

Student Name: Vishal Rajesh Mahajan **Student Roll No:** 1

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; extorting money from users via ransomware; or interrupting normal business processes.

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; but now, its scope has been enhanced to encompass all the latest communication devices.
- **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

1. Define Cyber Security.

Answer: Cyber security is the practice of protecting systems, networks, and data from digital threats through the use of strategies, tools, and frameworks designed to safeguard sensitive information and ensure the integrity of digital operations. It aims to establish multiple layers of defense across all potential access points covering data, software, hardware, and connected networks so that both organizations and individual users are defended against attacks intended to access, alter, destroy, or extort valuable data. Effective cybersecurity not only employs technical measures such as firewalls, intrusion detection systems, and security protocols, but also involves educating all users about security best practices, compliance, and how to detect and respond to emerging threats.

[**Source:** *https://www.techtarget.com/searchsecurity/definition/cybersecurity*]

2. Discuss different types of Cyber threats. (minimum 5)
Answer:

- **Malware attacks:** Software such as viruses, worms, Trojans, ransomware, and spyware designed to damage or gain unauthorized access to systems.
- **Advanced persistent threats (APTs):** Sophisticated, prolonged attacks often orchestrated by nation-states or organized crime groups to infiltrate networks and steal information.
- **Distributed denial-of-service (DDoS) attacks:** Overwhelm a system or network with excessive traffic, making it unavailable to users.
- **Man-in-the-middle (MitM) attacks:** Intercept communications between two parties to steal sensitive information or alter data.
- **Social engineering attacks:** Manipulate individuals into divulging confidential information, commonly through phishing, baiting, or pretexting

[**Source:** *https://www.sailpoint.com/identity-library/cyber-threats*]

3. What happens if anyone breaks a cyber-law?
Answer: If anyone breaks a cyber-law in India, they may face imprisonment and monetary fines, the severity of which depends on the nature of the offence. For example, hacking can result in imprisonment for up to three years and/or a fine up to ₹5 lakh, while serious acts like cyber terrorism can lead to life imprisonment. Other offences such as identity theft, publishing obscene material, or unauthorized access also carry significant penalties, including both jail terms and substantial fines
[**Source:***https://legaleye.co.in/blog_news/punishments-for-cyber-crime-under-indian-constitution/*]

4. Importance of Cyber Law and standards ?
Answer: Cyber law is highly important because it provides a legal framework for governing activities in the digital environment. It helps protect individuals and organizations from threats like hacking, identity theft, data breaches, and online fraud. Cyber law also ensures that personal and financial data are handled securely, which builds trust in digital transactions and promotes safe e-commerce practices. Additionally, these laws uphold intellectual property rights and require organizations to follow cybersecurity standards, helping to prevent misuse of technology and digital content. Overall, cyber law and standards are vital for maintaining order, security, and trust as society becomes increasingly reliant on the internet
[**Source:***https://www.simplilearn.com/what-is-cyber-law-article*]

5. What are the areas involved in Cyber Law?
Answer:
Areas involved in Cyber Law broadly cover legal aspects related to digital activities and online security. Key domains include:

- **Cybercrimes:** These comprise hacking, identity theft, phishing, cyber fraud, cyberstalking, ransomware attacks, and denial of service (DoS) attacks. Laws define these offenses and specify penalties such as imprisonment or fines. For example, hacking (unauthorized access to computer systems) and identity theft are punishable under specific sections of the IT Act in India.
- **Data Protection and Privacy**: Regulations that safeguard personal and sensitive data from unauthorized access or misuse, ensuring individuals' privacy rights in the digital space.
- **E-commerce and Digital Contracts:** Legal rules that govern online transactions, electronic signatures, and digital agreements to ensure validity and security in online business.
- **Intellectual Property Rights:** Protection against unauthorized distribution or reproduction of digital content, software, and inventions to encourage innovation.
- **Cyberterrorism and National Security**: Laws addressing the use of cyberspace for acts threatening national security, including attacks on critical infrastructure.
- **Digital Content Regulation**: Addressing unlawful or obscene content circulation, child pornography, hate speech, and online harassment or cyberbullying.

Overall, Cyber Law acts as a comprehensive regulatory system to protect users and organizations, facilitate secure digital commerce, and prevent misuse of technology in various forms.

[**Source:***https://www.sattrix.com/blog/cyber-law-in-india/*]

6. What are Standards you study in Cyber Law?
Answer:
Standards studied in Cyber Law primarily focus on establishing frameworks and best practices to ensure cybersecurity, data protection, and lawful digital conduct. These standards include:

- **Information Security Management Systems (ISMS):** Frameworks like ISO/IEC 27001 that define requirements for managing information security systematically.
- **Cybersecurity Guidelines and Best Practices:** Issued by regulatory bodies such as CERT-In in India and NIST in the U.S., these encompass network security, application security, data security, incident response, and vulnerability management.

- **Compliance and Reporting Standards:** Rules mandating timely reporting of cybersecurity incidents and breaches to authorities, such as CERT-In's 6-hour data breach reporting rule.
- **Data Protection Standards:** Policies to protect personal data privacy and ensure secure handling, aligned with laws and regulations.
- **Risk Management and Audit Procedures:** Standards that guide organizations in risk assessments, security audits, and continuous monitoring to maintain cyber resilience.

These standards help organizations implement robust security measures, comply with legal requirements, and protect critical systems and data from cyber threats.

[**Source:***https://www.sattrix.com/blog/cyber-law-in-india/*]

7. How to protect yourself on the Internet?
Answer: To protect yourself on the Internet, follow these essential practices:

- Keep software and systems updated: Regularly install updates and patches to fix security vulnerabilities.
- Use strong, unique passwords: Avoid password reuse; use a password manager to create and store complex passwords.
- Enable multi-factor authentication (MFA): Add an extra verification step to prevent unauthorized access even if passwords are compromised.
- Be cautious with links and attachments: Avoid clicking on suspicious or unsolicited links and attachments to prevent phishing attacks.
- Backup your important data: Use the 3-2-1 rule—keep three copies of data on two different media with one off-site backup.
- Use secure and private networks: Avoid public Wi-Fi without a VPN (Virtual Private Network) to protect your data from interception.
- Activate firewalls and security software: Firewalls control network traffic and security software protects against malware.
- Limit personal information sharing: Be mindful of what you share online and regularly review privacy settings on social media.

[**Source:***https://skillogic.com/blog/top-cyber-hygiene-essential-tips/]*

Post-Experiments Exercise

Extended Theory: Nil

Results/Calculations/Observations:

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/**