Cyber Security

Course Code: CSC5311 Course Title: Information Security Management

Dept. of Computer Science
Faculty of Science and Technology

Lecturer No:	2	**Week No:**		**Semester:**	Summer 24-25
Assistant Professor:	Dr. Rajarshi Roy Chowdhury (rajarshi@aiub.edu)				

Lecture Outline

1. Cyber Security
2. Importance of Cyber Security
3. Cyber Security Domains
4. Tools and Technologies
5. Best Practices for Cyber Security
6. Cyber Laws and Regulations
7. Career Opportunities in Cyber Security
8. Future of Cyber Security

What is Cyber Security ?

- Cyber Security is the practice of protecting systems, networks, and data from digital attacks.
- Focuses on confidentiality, integrity, and availability (**CIA Triad**).
- Important in personal, business, and government sectors.
- It is a **multidisciplinary domain** involving computer science, information security, risk management, cryptography, and legal/regulatory compliance.

Importance of Cyber Security

Protects sensitive data from theft or misuse.

Prevents financial loss due to cybercrime.

Ensures trust and credibility of businesses.

Supports national security and critical infrastructure.

Types of Cyber Threats

- Malware: Viruses, worms, ransomware, spyware.
- Phishing: Fraudulent attempts to obtain sensitive information.
- Denial-of-Service (DoS): Overwhelming a system to make it unavailable.
- Man-in-the-Middle Attacks: Intercepting communication between two parties.
- Zero-day Exploits: Attacks on unknown vulnerabilities.

Cyber Security Domains

- Network Security – protect the CIA of data
- Application Security - securing software applications by identifying and fixing vulnerabilities
- Endpoint Security - securing end-user devices
- Data Security - protecting data at rest, in transit, and in use from unauthorized access or corruption
- Identity and Access Management - ensuring the AAA properties
- Cloud Security
- Mobile Security

Tools and Technologies

- Firewalls
- Antivirus and Anti-malware
- Encryption tools
- Intrusion Detection Systems (IDS)
- Multi-Factor Authentication (MFA)
- Security Information and Event Management (SIEM) systems

Best Practices for Cyber Security

Use	Use strong, unique passwords and change them regularly.
Enable	Enable two-factor authentication.
Update	Update software and systems regularly.
Avoid	Avoid clicking on suspicious links or attachments.
Back up	Back up data regularly.
Educate	Educate users on security awareness.

Cyber Laws and Regulations

- General Data Protection Regulation (GDPR)
- Computer Fraud and Abuse Act (CFAA)
- Cybersecurity Act
- Digital Security Act (Bangladesh)
- Importance of compliance and ethical responsibility

Career Opportunities in Cyber Security

- Security Analyst
- Penetration Tester (Ethical Hacker)
- Security Architect
- Chief Information Security Officer (CISO)
- Forensic Expert
- Security Software Developer

Future of Cyber Security

- AI and Machine Learning for threat detection
- Quantum computing and encryption challenges
- Increased focus on privacy and data ethics
- Cybersecurity in IoT and smart devices
- Global cooperation against cybercrime

Recommended Books

Books

1. **Information Security Management Handbook** (6th Edition), Harold et al.
2. **Information Security and IT Risk Management**, Manish et al.
3. Random online resources