**CSE487: Cyber Security, Law, and Ethics**

**Instructor: Dr. Md. Hasanul Ferdaus**

PhD (Monash University), MS (KIT, Germany & Polito, Italy), BSc (CSE BUET)

**Assistant Professor**

**Department of CSE, East West University**

**Former Faculty Member, Monash University and CQ University, Australia**

**Former Researcher, Melbourne University, Australia**

**Former Researcher, KIT and FZI, Germany**

**Lecture 1 Introduction to Cyber Security**

The purpose of cybersecurity is to safeguard internet-connected devices and services from malevolent attacks initiated by hackers, spammers, and cybercriminals. This protective measure is commonly employed by companies to shield themselves against a variety of threats, such as phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses.

If you observe the present-day society, you'll notice that our daily lives are increasingly reliant on technology. This dependence brings numerous advantages, including quick access to online information and the convenience offered by smart home automation and concepts like the Internet of Things (IoT).

However, amidst the positive aspects, it is important to acknowledge the existence of potential threats that lie within each device and platform. Despite the generally optimistic view of technological progress, cyber security threats posed by modern technology are indeed a tangible danger.

# What is Cyber Security

Cyber security is a discipline that covers how to defend devices and services from electronic attacks by nefarious actors such as hackers, spammers, and cybercriminals. While some aspects of cyber security involve proactive measures, the majority of professionals in this field focus on determining the most effective ways to safeguard all assets, ranging from computers and smartphones to networks and databases, against potential attacks.

In the media, the term "Cyber Security" is often used broadly to describe protection against various forms of cybercrimes, including identity theft and international digital warfare. According to Cisco Systems Inc., a prominent technology conglomerate specializing in networking, Cloud Computing, and security, Cyber Security is defined as: "The practice of protecting systems, networks, and programs from digital attacks. These cyberattacks typically aim to gain unauthorized access, manipulate or destroy sensitive information, extort money from users, or disrupt normal business operations."

# Why is Cybersecurity Important?

In the present era of technology, the importance of cybersecurity cannot be underestimated. A mere instance of security breach can result in the exposure of personal data belonging to countless individuals. Such breaches not only carry significant financial implications for companies but also causes a great loss of trust of their customers. Therefore, it is crucial to prioritize cybersecurity in order to safeguard businesses and individuals against the threats posed by spammers and cybercriminals.

# Scale of Cyber Security Threats

As stated by Cybercrime Magazine1, it is projected that cybercrime will result in an annual cost of 10.5 trillion USD worldwide by 2025. Additionally, the global expenses associated with cybercrime are anticipated to increase by approximately 15 percent each year over the next four years2.

1 <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>

2 <https://www.thenationalnews.com/business/technology/2021/12/29/top-10-cyber-crime-trends-to-watch-out-for-in-2022/>

Various factors, including the pandemic, the prevalence of cryptocurrency, and the growing trend of remote work, are converging to create a fertile ground for criminals to exploit. These factors contribute to an environment that presents numerous targets for cybercriminals to take advantage of.

# Scope of Cyber Security

Cybersecurity involves the utilization of technologies, procedures, and approaches to safeguard computer systems, data, and networks against malicious attacks. In order to provide a comprehensive understanding of what cybersecurity entails and how it operates, we need to break it down into several subdomains.

## Application Security

Application security focuses on implementing various protective measures within an organization's software and services to counter a wide range of threats. This particular area necessitates the expertise of cybersecurity professionals to develop secure code, design secure application structures, establish rigorous data input validation, and perform other tasks aimed at reducing the risk of unauthorized access or alteration of application resources.

## Identity Management and Data Security

This particular area encompasses actions, frameworks, and procedures that facilitate the verification and validation of legitimate individuals accessing an organization's information systems. These measures involve the implementation of robust data storage mechanisms to safeguard information, whether it is in transit or stored on servers or computers. Furthermore, this subdomain emphasizes the utilization of authentication protocols, such as two-factor or multi-factor authentication, to enhance security.

## Network Security

Network security pertains to the hardware and software components employed to safeguard the network and infrastructure against disruptions, unauthorized entry, and various forms of misuse. By implementing robust network security measures, organizations can effectively shield their assets from a diverse array of threats, whether originating from internal or external sources.

## Mobile Security

In today's world, the importance of mobile security cannot be overstated due to the increasing dependence on mobile devices. This particular field focuses on safeguarding both personal and organizational data stored on devices such as tablets, cell phones, and laptops from various risks, including unauthorized entry, device misplacement or theft, malware, viruses, and more. Furthermore, mobile security utilizes authentication and educational measures to enhance overall security.

## Cloud Security

Cloud security involves the establishment of secure cloud architectures and applications for organizations that utilize cloud service providers such as Amazon Web Services, Google Cloud, Microsoft Azure, Rackspace, and others.

## Disaster Recovery and Business Continuity Planning

Not all risks stem from human actions. The Disaster Recovery (DR) and Business Continuity (BC) subdomain encompasses procedures, notifications, monitoring, and strategies devised to assist organizations in preparing for the continuity of their business-critical systems during and after various incidents, such as extensive power outages, fires, or natural disasters. It aims to facilitate the resumption and recovery of operations and systems that may have been compromised or disrupted as a result of the incident

## User Education

Information is a valuable asset, and the knowledge of cyber threats among staff plays a crucial role in the overall cybersecurity framework. Providing comprehensive training to business personnel on the fundamentals of computer security is vital for promoting awareness about industry best practices, organizational procedures and policies, as well as recognizing, monitoring, and reporting suspicious or malicious activities. This subdomain encompasses cyber security-oriented courses, programs, and certifications aimed at enhancing staff expertise in this field.

# References

[1] Book: Cryptography and Network Security, William Stallings, Chapter 1.

[2] <https://www.simplilearn.com/tutorials/cyber-security-tutorial>

[3] <https://www.geeksforgeeks.org/cyber-security-tutorial/>

[4] <https://www.simplilearn.com/tips-for-securing-the-cloud-article>