**Cyber security Course Report:**

**Why Cyber Security?**

Cyber-attacks are a great threat to global economy as well as to our personal data.

In 2015, a computer security group Vera code reported that defending UK businesses against cyber-attacks and repairing the damage done by hackers costs businesses £34 billion per year.

There are two important aspects that need to be protected:

1. Information: Customer's data, source code, design documents, financial reports, employee records, intellectual property, etc.

2. Information systems: Computers, Networks, cables etc.

A good Cyber security approach plays a vital role in minimizing and controlling damage, recovering from a Cyber-breach and its consequences.

**What is Cyber Security?**

Cyber Security is a set of techniques used to protect systems, networks, and applications from attacks, damage or unauthorized access emerging from internet.

These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

With comparatively more devices than people around, implementation of effective Cyber Security measures is a challenge in today's world.

According to Forbes, the IT security spending is expected to reach around $170 billion on Cyber Security solutions by the year 2020.

**Categories of Attacks**

Information security involves protecting information systems from various types of attacks, including:

Malware Attacks: Involving malicious software such as viruses, worms, and ransom ware.

Phishing Attacks: Where attackers trick individuals into providing sensitive information.

Denial-of-Service (DoS)Attacks: Overwhelming systems to make them unavailable to users.

Man-in-the-Middle (MitM) Attacks: Intercepting and altering communications between parties.

SQL Injection Attacks: Exploiting vulnerabilities in databases to access and manipulate data.

**Objectives of Cyber security:**

Each of these attacks violates a specific desired property of security. These properties are termed as **security objectives**. Security objectives are also known as security goals, characteristics of information and information systems.

The three standard pillars (Security Objectives) of Cyber security are:

1. **Confidentiality**

* Makes sure that data remains private and confidential. It should not be viewed by unauthorized people through any means

1. **Integrity**

* Assures that data is protected from accidental or any deliberate modification

1. **Availability**

* Ensures timely and reliable access to information and its use.

These three principles are together called as the **CIA**(**C**onfidentiality, **I**ntegrity and **A**vailability) triad. An alternate way of referring CIA is through **DAD**(**D**isclosure, **A**lteration and **D**enial) triad.

There are three more important concepts in information security to support these pillars known as **AAA**(**A**uthentication, **A**uthorization and **A**ccounting) services. These services are used to support the CIA principles.

1. **Authentication**

* Authentication is verifying an identity

1. **Authorization**

* Authorization isdeterminingwhether a particular user is allowed to access a particular resource or function

1. **Accounting (Non-repudiation)**

* Accounting includes two other components - auditing & non-repudiation
  + Auditing is recording a log of activities of a user in a system
  + Accounting refers to reviewing the log file to check for violations and hold users answerable to their actions. It includes non-repudiation

Having learnt about the objectives and services of Cyber Security, let us get familiar with other commonly referred Terms of Cyber Security.

**Conclusion**

An overview of the field of cyber security was provided.

The size and simplicity of this course should not lead one to think cyber security is a small field.

Cyber security is vast field with many domains like application security, data security, and identity and access management. Each of these is specializations with cyber security and these domains themselves might have further sub-domains/sub-specializations.

You can view the org chart of the Information Security Group (ISG) in Infosys by going to Sparsh -> Units in Infosys -> Information Security Group -> Org Chart (available only in Infosys Intranet), to get an idea of how vast the field is and the various specializations and sub-specializations with it.







