**What will you learn?**

1. What is Cybersecurity?

2. Cybersecurity Fundamentals

3. Types of Cyber Attacks

4. Cybercrime

5. The Future of Cybersecurity

**What is Cybersecurity?**

Cyber security is a branch of security that focuses on protecting systems, networks, computers, and data, from unauthorized access (intentional and unintentional), modification, or destruction.

**Importance of CyberSecurity**

It is estimated that approximately 1 million potential cyberattacks are attempted per day, and with the evolution of mobile and cloud technologies, this number has the likelihood to increase.

The range of operations of cyber security involves protecting systems, applications, and data from major cyber threats. However, cyberthreats have become increasingly more innovative and the need for proper cyber defense to protect our data has never been more important.

**Cybersecurity Fundamentals**

**The CIA Triad**



The CIA triad (not to be confused with the US Central Intelligence Agency) is a security concept that guides the development of security systems and policies within an organization.

**Confidentiality**

Confidentiality is defined as the act of preventing the disclosure of data to unauthorized parties. It also means ensuring that the identity of authorized parties involved in sharing and holding data is kept private and anonymous.

Cracking poorly encrypted data and disclosing sensitive data are among the most common ways that confidentiality can be compromised.

Standard measures to establish confidentiality include:

* Data encryption
* Two-factor authentication
* Biometric verification
* Security tokens

**Integrity**

This refers to the ability to protect a system and its information from being modified by unauthorized parties. A common integrity violation is when a [cyber attacker](https://itlaw.wikia.org/wiki/Attacker) [encrypts](https://searchsecurity.techtarget.com/definition/encryption) [sensitive](https://itlaw.wikia.org/wiki/Sensitive) or important corporation information and demands a ransom for the [data](https://itlaw.wikia.org/wiki/Data) to be restored. This is called [ransomware.](https://itlaw.wikia.org/wiki/Ransomware)

Standard measures to guarantee integrity include:

* Cryptographic checksums
* Using file permissions
* Uninterrupted power supply
* Data backups

**Availability**

This refers to the ability to guarantee that authorized parties can access systems, programs, and information when needed. The most common attack that impacts availability is Denial-of-Service(D-o-S) in which the attacker makes a system or network resource unavailable to legitimate users.

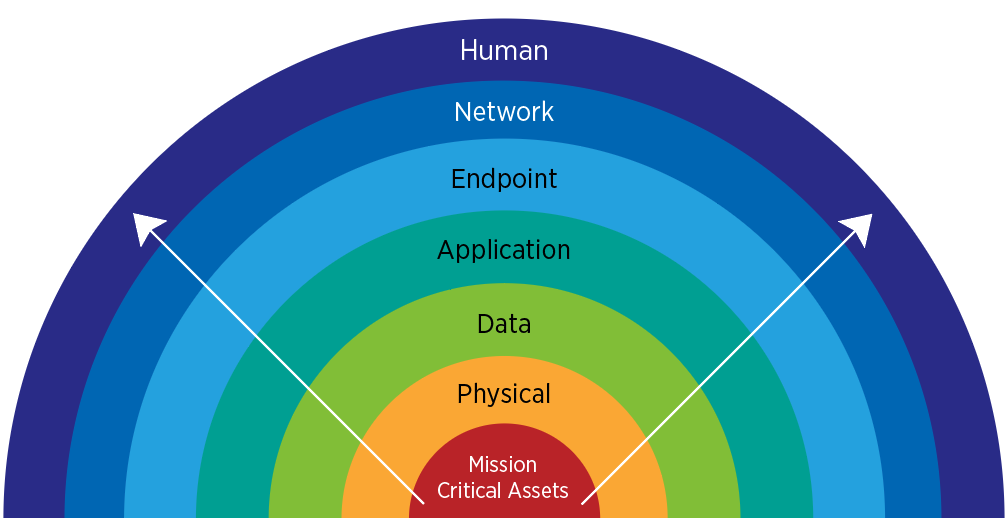
The concept involves flooding a network with more traffic than it can handle which eventually leads to a crash.

Standard measures to guarantee availability include:

* Backing up data to external drives
* Implementing firewalls
* Having backup power supplies
* Data redundancy
* Network monitoring

**Layered Cybersecurity Approach**

While every company system and network is different, the layered cybersecurity model strives to serve as a basis for which companies can lay their security policies.



* **Mission Critical Assets**

These are systems, applications, and data whose failure, disruption or if compromised would cause a major crisis within the organization.

* **Physical Security**

This security layer addresses security concerns in regards to the physical properties of a system. This includes the physical cutting of cables, natural disasters, and other forms of human vandalism.

* **Data Security**

This involves the security controls in charge of the storage and transfer of data.

* **Application Security**

This layer protects and controls access to an application, an application’s access to the mission-critical assets, and the internal security of the application.

* **Endpoint Security**

This ensures that the connection between endpoints of user devices and the network is not vulnerable to breaches or exploitation.

* **Network Security**

This protection layer controls and prevents unauthorized access to the network.

* **Human Layer**

We are the weakest link in any cyber security posture. Human security controls protect mission-critical assets from a variety of human threats, including cybercriminals, malicious insiders, and negligent users.

**Types of Cyberattacks**

A cyber-attack can be defined as any deliberate attempt to gain unauthorized access to a computer system, application, or network with malicious intent.

There are various ways to classify cyber-attacks, however, in this lesson, we will stick to two broad categories:

a. System-based attacks

b. Web-based attacks

**System-based Attacks**

These are the attacks that are intended to compromise a computer system or a network system. Below are some common system-based attacks:

**Virus**

It is a malicious software program that when executed, spreads throughout the computer files without the knowledge of a user. It can also carry out commands to harm the system.

**Worm**

This is malicious software similar to a computer virus. However, a major difference between the two is that a virus is activated when triggered by its host while a worm propagates and self-replicates independently.

**Trojan Horse**

It is a malicious program that is often disguised as legitimate software but when opened/executed malicious code will run in the background and allow cybercriminals backdoor access to the users’ system.

**Backdoors**

It is a form of trojan that facilitates remote unauthorized access to a user’s computer system or network. Sometimes backdoors have legitimate use like granting access for troubleshooting.

**Bots**

A bot is a script or software program that runs automated tasks while imitating/replacing human user behavior. Some bots programs run automatically, while others only execute commands when they receive specific input.

**Web-based Attacks**

These are the attacks that occur on a website or web application.  Below are some common system-based attacks:

**Injection attacks**

It allows an attacker to inject malicious code into a network/program/query and fetch data from the database to the attacker. This type of attack also allows an attacker to inject malware to execute commands remotely.

**DNS Spoofing**

DNS Spoofing is a type of computer security hacking. Whereby data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker’s computer or any other computer. The DNS spoofing attacks can go on for a long period without being detected and can cause serious security issues.

**Session Hijacking**

It is a type of cyber attack where an attacker takes over a user session over a protected network. An attacker steals web cookies to have access to user data collected from sessions.

**Phishing**

Phishing is a type of attack where an attacker disguises themself as a trustworthy entity and attempts to steal sensitive information like user login credentials and credit card numbers.

**Brute Force**

It is a type of attack which uses a **trial-and-error** method. This attack generates a huge number of guesses and validates them to obtain actual data like personal user information. This attack may be legitimately used to crack encrypted data, or by security, analysts to test an organization's network security.

**Denial of Service**

It is an attack meant to trigger a system crash by flooding the targeted traffic with information rendering the server or network resource unavailable to the users. It uses a single system and a single internet connection to attack a server.

It can be classified into the following:

**a) Volume-based attacks** whose goal is to saturate the bandwidth of the target site and magnitude is measured by bits/second.

**b) Protocol attacks** whose goal is to consume actual server resources and is measured in packets/second.

**c) Application layer attack** whose goal is to crash the web server and is measured in request/second.

**Dictionary Attacks**

This type of attack stored the list of commonly used passwords and validated them to get the original password.

**URL Interpretation**

It is a type of attack where we can change certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

**File Inclusion Attacks**

It is a type of attack that allows an attacker to access unauthorized or essential files which are available on the webserver or to execute malicious files on the web server by making use of the included functionality.

**Man in the Middle Attacks**

It is a type of attack that allows an attacker to intercept the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

**Other terms:**

**Cyber threats** are security incidents or circumstances with the potential to have a negative outcome for your network or other data management systems.

Examples of common types of security threats include phishing attacks that result in the installation of malware that infects your data, failure of a staff member to follow data protection protocols that cause a data breach, or even a tornado that takes down your company’s data headquarters, disrupting access.

Attacks are threats that have been carried out in either of the categories below:

**a) Passive** – Make use of information from the system without affecting system resources

**b) Active** – Alter system resources or affect the operation

**OR**

**a) Insider** – Initiated by an entity inside the organization

**b) Outsider** – Initiated from outside the perimeter

**Vulnerabilities** are the gaps or weaknesses in a system that make threats possible and tempt threat actors to exploit them.

The most common types of vulnerabilities include OS Command Injection, SQL injections, server misconfigurations, cross-site scripting, and transmitting sensitive data in a non-encrypted plain text format.

Vulnerabilities can be categorized in three ways:

* Corrupted (Loss of integrity)
* Leaky (Loss of confidentiality)
* Unavailable or very slow (Loss of availability)

**Remember**

**Threats** represent “potential security harm to an asset” when **vulnerabilities** are “exploited”.When threat probability is multiplied by the potential loss that may result, cyber security experts, refer to this as a **risk**.

**Cybercrime**

The term **cybercrime** is used to describe an unlawful activity in which computer or computing devices such as smartphones, tablets, etc. which are stand-alone or a part of a network are used as a tool or/and target of criminal activity.

Cyber security risks arise from three types of actions:

i) Inadvertent actions (generally by insiders) that are taken without malicious or harmful intent.

ii) Deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to harm.

iii) Inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action.

To better understand cyber criminals, we have attempted to categorize them based on their motives; of which there are three categories of motivation.

* **Political motivations**: Examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.
* **Economic motivations**: Examples include theft of intellectual property or other economically valuable assets (e.g., funds, credit card information); fraud; industrial espionage and sabotage; and blackmail.
* **Socio-cultural motivations**: Examples include attacks with philosophical, theological, political, and even humanitarian goals. They also include fun, curiosity, and a desire for publicity or ego gratification.

Some cybercriminals are organized, use advanced techniques, and are highly technically skilled. Others are novice hackers.

**Cybersecurity Tips**

**The old firewall solution**

There are limitations to its blocking capabilities, the firewall is still a good tool that you can use to filter your Internet traffic, and block communication from an infected machine or online location.

**Get a good antivirus**

You still need a good antivirus to catch most malware, block phishing threats and check the web reputation of popular online domains.

**Use Anti-spyware solutions**

Spyware is software that monitors your Internet traffic and uses your personal information against you. To stay safe from spyware, there are a few popular anti-spyware products, like Malwarebytes or Spybot Search and Destroy that you can choose from.

**Use automatic update tools for vulnerable applications**

By using security holes in unpatched applications, cybercriminals manage to spread exploits that deliver financial and data-stealing malware on the affected systems.

For this reason, it is important to have the most up-to-date security patches available and this may be done by using a free solution that automatically updates your system.

**Use a password manager**

It is easy to forget the numerous passwords you have set. To avoid this issue, most people simply choose to use only one or two passwords all the time.

But, this makes you vulnerable to hackers because all they need to do is to crack your password and have access to all your online accounts.

That’s because not all these online accounts incorporate high-security standards to protect our passwords. A password manager is the safest bet to keep all your unique passwords.

**Backup your system and sensitive information**

To keep sensitive information secure from cyber-criminals, a backup solution is the best option you have. So, in case your system is blocked by ransomware that stops you from accessing it, you’ll format the system and use your backup to restore it.

You can use one of the available backup solutions or you can keep the most important data in the cloud and access it from any location and any device.

**Encrypt your important files**

By encrypting your personal information you ensure cybercriminals will not access your confidential data, even if they gain access to your OS. You can also encrypt files on your local disk or on an online location, which makes things harder for any hacker.

**Protect your online traffic by using multiple tools**

Use a VPN solution to encrypt your online connection or Use the Tor browser that allows you to browse the internet anonymously by sending your communication through the Tor network of computers.

However, to improve your online protection, you cannot rely on a single solution, you rather need to understand that multiple means and guidelines need to be followed.

**Stay up-to-date on Cybersecurity tools**

While you may consider yourself presently cyber-secure by applying all these tips, future events may change your opinion. Learn to adopt new tools to protect against phishing attempts, spam campaigns, malicious web pages, and cybercriminal attacks.

**The Future of Cybersecurity**

Presently, the need for better cyber security methods has reached all-time high importance because of ever-increasing cyber threats. The evolution of cyber threats and their scale of destruction in recent years has brought about a change in the perception of cyber security and proven the need for an active and dynamic cyber security infrastructure.

While providing cybersecurity for large entities such as the government is becoming harder, Individuals should take precautions such as using licensed antivirus software, using an active firewall, not entering untrusted websites, not downloading any files from untrusting websites, and not sharing every information everywhere. Individuals should use websites that’s URL addresses start with “HTTPS” and they should scan their files.

The most important factor in cyber security is “**human**”. Humans are the weakest link of cyber security. Therefore, providing training about cyber security to users of computer technologies should be a priority.

Although there is no way to know precisely what the future of cybersecurity holds, it will likely be full of innovation and improvements. As technology advances, so does the need for better cybersecurity solutions.

The demand for Cyber Security professionals has increased significantly in the last few years making a career in cybersecurity very promising.