**WEEK 01**

**BRIEF HISTORY AND TYPES OF CYBER SECURITY**

Cyber Security is the practice of Protecting computers, mobile devices, Servers, electronic Systems, networks, and data from malicious attacks. It is also known as Information Security (INFOSEC) or Information Assurance (IA), System Security. The first cyber malware virus developed was pure of innocent mistakes. But cybersecurity has evolved rapidly because of the impeccable increase in the cybercrime law field on the Web.

*Cyber Security* is all about protecting your devices and network from unauthorized access or modification. The Internet is not only the chief source of information, but it is also a medium through which people do business.

Cybersecurity is becoming increasingly significant due to the increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of smart devices and the various devices that constitute the ‘Internet of things’.

Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world. Where did it all begin? We take a look at the history of cybersecurity from inception to the present day.

**Types of cyber security**

Cyber security is a wide field covering several disciplines. It can be divided into seven main pillars:

[Application security](https://www.synopsys.com/software-integrity/security-testing.html) involves implementing various defenses within all software and services used within an organization against a wide range of threats. It requires designing secure application architectures, writing secure code, implementing strong data input validation, threat modeling, etc. to minimize the likelihood of any unauthorized access or modification of application resources.

**1. Network Security**

Network security is a set of technologies that protects the usability and integrity of a company's infrastructure by preventing the entry or proliferation within a network of a wide variety of potential threats

Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption and more.

**2. Cloud Security**

Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data, and infrastructure. These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.

**3. Endpoint Security**

Endpoint security is the practice of securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns. Endpoint security systems protect these endpoints on a network or in the cloud from cybersecurity threats. Endpoint security has evolved from traditional antivirus software to providing comprehensive protection from sophisticated malware and evolving zero-day threats.

**4. Mobile Security**

Mobile Device Security refers to **the measures designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices**. At the root of mobile device security is the goal of keeping unauthorized users from accessing the enterprise network.

**5. IoT Security**

Internet of things (IoT)security is **the practice of securing IoT devices and the network these devices use**. Its primary goals are to maintain the privacy of users and confidentiality of data, ensure the security of devices and other related infrastructures, and allow the IoT ecosystem to function smoothly.

[IoT security](https://www.checkpoint.com/solutions/iot-security/) protects these devices with discovery and classification of the connected devices, auto-segmentation to control network activities, and using IPS as a virtual patch to prevent exploits against vulnerable IoT devices. In some cases, the firmware of the device can also be augmented with small agents to prevent exploits and runtime attacks.

**6. Application Security**

Application security is **the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification**.

**7. Zero Trust**

Zero Trust is **a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction**.

The traditional security model is perimeter-focused, building walls around an organization’s valuable assets like a castle. However, this approach has several issues, such as the potential for insider threats and the rapid dissolution of the network perimeter.\

**The Purpose of Cybersecurity**

The [purpose of cyber-security](https://wilsoncgrp.com/) is to prevent data breaches, identity theft and cyber-attacks as well as risk management in some cases. When an enterprise applies an effective incident response plan and has a strong network security, it is better positioned to mitigate and prevent cyber-attacks. For instance, end user protection guards against theft or loss of information while scanning computer devices for malicious codes. In light of this, organizations and the cyber-security stakeholders must remain up-to-date with the emerging technologies, threat and security intelligence trends in order to design the ideal cyber-security measures

This helps to ensure that all internet connected assets and information are secured from cyber-threats that take many forms such as;

**Ransomware:**it is deployed by an attacker in the form of a malware that locks a target’s computer system and files through encryption. The attacker demands a lump sum payment in order to decrypt and unlock the computer systems and files.

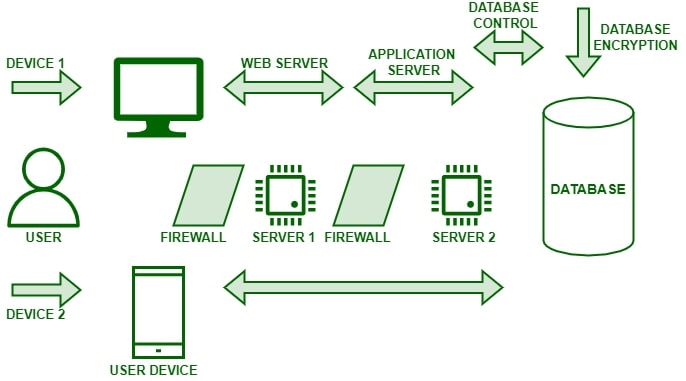
**Malware:**this is any program or file that is deployed with the aim of harming a computer user like; computer virus, worms, spyware and Trojan horses.

**Social engineering:** this is a new form of cyber-attack that is executed through tricking system users into breaching security procedures to grant the attackers access to sensitive and private business information that is protected.

**Phishing:**this is a type of cyber fraud that entails sending out fraudulent emails that bear a resemblance to emails from reputable sources. However, the fraudulent emails are designed to steal sensitive user information such as login information and credit card details.

**IMPORTANCE OF CYBER SECURITY**

* Cybersecurity is just an ethical practice to protect our devices from such hackers and make them more secure. People involved in cybersecurity perform security measures and operations in order to keep our data and devices safe. Cybersecurity basically deals with protecting our network, devices, and data from illegal and unauthorized access by other people. Hackers and cybercriminals use the Internet as an opportunity to crack into other’s people devices by using spyware, malware and carrying out cyber attacks.
* The main purpose of Cybersecurity is to protect all the users on the Internet from infected files, malware, and digital attacks which lead the users to access private sensitive information of users, extort ransom from users by using their private data or even disrupting important critical infrastructure like shutting down power supplies and military infrastructure.
* [Cybersecurity](https://www.geeksforgeeks.org/cyber-security-types-and-importance/) helps to solve pre-built vulnerabilities in applications and helps them to remain stable throughout. More and more devices are getting connected to the Internet, hence it is more and more important to secure all the devices over the Internet to protect them all against unauthorized access.



* Communicate data breaches
* Appoint a data protection officer
* Require user consent to process information
* Anonymize data for privacy

**CHALLENGES OF CS**

* Increased unlawful use of networks
* Increasing attacks on mobile devices and IoT devices
* Manipulating Artificial Intelligence systems or bypassing machine learning implementations
* Use of advanced AI by hackers
* An increase in ransomware and spyware in the market
* Not enough research is being conducted on lesser-known threats and emerging threats
* Cyber attacks can occur out of nowhere and from anywhere. Multiple sources and vectors can be used for attacks
* Phishing and spear-phishing
* Lack of education regarding cyber security and protecting devices
* Hacktivism and cyberterrorism are growing extensively
* Dronejacking and other modern methods
* Advanced social engineering
* Multiple vendors, partners, and employees have access to systems and data, thus increasing the number of sources and vectors again

**APPLICATIONS**

* Business protection against cyberattacks and data breaches.
* Protection for data and networks.
* Prevention of unauthorized user access.
* Improved recovery time after a breach.
* Protection for end users and endpoint devices.
* Regulatory compliance.

### 1. Network Security Surveillance

Continuous network monitoring is the practice of looking for indications of harmful or intrusive behavior. It is often used in conjunction with other security tools like firewalls, antivirus software, and IDPS. Monitoring for network security may be done manually or automatically using the software.

### 2. Identification And Access Control (IAM)

The management has control over which individual can access which sections of the data. Usually, the management regulates who has access to data, networks, and computer systems. Here is where cybersecurity comes into the picture by identifying users and executing an access control. Various cyber security applications ensure IAM across an organization. IAM may be implemented in both software and hardware, and it often makes use of role-based access control (RBAC) to limit access to certain system components.

### 3. Software Security

Applications that are crucial to company operations are protected by application security. It contains controls like code signing and application whitelisting and may assist unify your security rules with things like file sharing rights and multi-factor authentication. With the application of AI in cyber security, software security is bound to increase.

### 4. Risk Management

Risk management, data integrity, security awareness training, and risk analysis are all covered by cyber security. The evaluation of risks and the control of the harm that may be done as a result of these risks are important components of [risk management](https://www.knowledgehut.com/blog/project-management/risk-management).

### 5. Planning for disaster recovery and business continuity

Data recovery enables organizations to continue working in the event of data loss, assaults, or calamities. By regularly data backup and spending money on a system that will enable corporate activities to continue, this application offers models or techniques that may help firms manage with severe data loss.

### 6. Physical Security

System locks, intrusion detection systems, alarms, surveillance systems, and data-destruction systems are a few examples of physical security measures. These allow organizations to secure their IT infrastructure.

### 7. Compliance And Investigations

Cybersecurity is helpful during the examination of suspicious situations. Additionally, it helps to upkeep and adhere to regulations.

### 8. Security During Software Development

The software aids in detecting software flaws when they are being developed and ensuring that regulations and standards are followed. Cybersecurity tools thoroughly test, scan, and analyze the software to identify any bugs, openings, or weaknesses that might be exploited by hackers or competing businesses.

### 9. Security Against DDoS

Cybersecurity aids in providing a mitigation solution to deal with DDoS. It redirects traffic to other cloud-based servers and resolves the issue.

### 10. Protecting Critical Systems

Cybersecurity aids in preventing assaults on huge servers linked to wide-area networks. It upholds the industry-standard, strict safety standards for users to abide by cybersecurity precautions to secure the devices. It keeps track of all apps in real-time and routinely evaluates the network security, servers, and users themselves.

**HOW DOES CYBER SECURITY WORKS**

This type of security **uses hardware and software to protect any data that's sent through your computer and other devices to the network**. Network security serves to protect the IT infrastructure and guard against information being intercepted and changed or stolen by cybercriminals

Cyber security is a complex field, and many roles can be found within **banks, retailers, e-tailers, healthcare, and government organizations**.