Case Study: To Study Cyber Security, its Needs and Application in various Domains.

What Is Cyber Security?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Need of Cyber Security:

Cyber security protects the data and integrity of computing assets belonging to or connecting to an organization’s network. Its purpose is to defend those assets against all threat actors throughout the entire life cycle of a cyber attack.

Applications of Cyber Security:

1. Backup and Data Recovery

You have back-ups of all your data. You’re safe, right? Maybe, but think about where that backed up information lives. Having backups of your data is only half the battle. We recommend a hybrid cloud-based backup model, meaning that backups are saved locally and in the cloud. **Hybrid cloud** backups offer better protection because you have three sets of data: production, local and off-site. Having your backup stored in the cloud can help you recover faster. Tape backup involves a lot of steps to recovery —retrieving the tapes, finding the data

you need on the tape, and loading it. Recovering your data from the cloud is quick and limited only by your bandwidth. Cloud backups are also safe from widespread disasters in your area, like a hurricane or flood.

2. Physical Access Controls

Controlling access to your campus, building and areas that contain sensitive data is a high security concern. It is critical to ensure that only authorized individuals have physical access to these areas. Access controls such as photo ID badges, least-privilege permissions for badge access, security cameras, a policy that requires guest check-in, are all important examples of physical access controls your business should consider implementing.

3. Logical Access Controls

It's not enough to simply restrict access to full-time company employees. It is also critical to ensure that only authorized individuals have access to your network and your data. Controls such as least-privilege permissions for end-user access to the network, periodic reviews of access permissions, and the immediate removal of access due to role change or termination are especially important to a comprehensive security plan. You should also require complex passwords for all employees with at least 10 characters and a combination of lower case letters, upper case letters, numbers and special characters. And, businesses should require a password change every 30-90 days.

4. Securely Configured and Encrypted Devices

Make sure all your end-user devices run secure, supported operating systems and have updates and patches applied as soon as they're available. What's the use of diligence in protecting access to your sensitive data if employees are utilizing unsecure mobile devices that easily access your network?

Here are a few device management tips:

- Laptops should be whole-disk encrypted in case they are lost or stolen.
- Tablets and cell phones that access company data need mobile device management to force a screen lock if they are lost or stolen.
- Antivirus should be running on all computers and laptops.

5. Securely Configured Network Components

A properly configured firewall is a critical part of perimeter security. Changes to the firewall need to be evaluated for security vulnerabilities. Refrain from using default passwords with network equipment, and change passwords immediately after support personnel are terminated.

6. Network segmentation

By utilizing network segmentation, your network is partitioned into multiple segments that can have limited access to each other. By limiting the access between network segments on the network, risk is mitigated from attacks like “land and expand” ransom ware variants.

7. Email and Online Protection

At least 91% of hacks begin with a phishing email! With this in mind, it is imperative to have weapons-grade email filtering in place that can block external emails that spoof your domain. We also recommend the practice of “sandboxing,” which is creating a protected environment in which to open and test file attachments and URLs. This is most commonly used as part of email filtering but can also be established in other services such as general web browsing. Restrict web use to only Firefox or Chrome – sorry Internet Explorer. Additionally, using a service such as Cisco’s Umbrella will block access to known malware sites, and even if one of your users clicks a potentially malicious link, it won’t be able to access the site.

8. Wireless security

Most companies supply their visiting customers or vendors with access to Wi-Fi. But, that doesn’t mean you need to give them keys to the executive suite. Set up a separate guest wireless connection. This prevents unauthorized access to your network.When setting up those wireless access points, change the SSID from the factory default, and use a complex password.