Section- 2

Q.1 Cyber Security:-

1. Cyber security refers to the protection of data and information from unauthorized access on the internet

2. Cyber Security is meant for proactive detection of loopholes in the security policies of the Computer System.

3. Cyber security defines the mechanism to extend operational support for management and protection of cyber dependent operations

Security Threat:-

Security threat is defined as a risk that which can potentially harm Computer System and ~~organism~~ organization. The Cause Could be physical such as Someone stealing a Computer that Contains vital data. The cause could also be non-physical such as a virus attack.

~~In these~~

Internal:- The threats include fire unstable power supply, humidity in the room housing the

hardware etc

External! These threats include lighting floods earthquakes etc

Human! These threats include theft Vandalism of the infrastructure and/or hardware disruption, accidental or Intentional errors.

Q.2

There are quite a few different networking Security tools you can incorporate into your line-up of services. The following list is by no means exhaustive but available security tools can include.

1. Access Control!- This refers to controlling which users have access to the network or especially sensitive section of network.

2. Antivirus and anti-malware Software

"malware or "malicious Software", is common form of cyberattacks that comes in many different shapes and size.

- **Application Security:-**

Each device and software product used within your network environment offers a potential way in for hackers.

- **Behavioral analytics:-** In order to identify abnormal behavior, security support personal need to establish a baseline of what Constitute.

- **Data loss prevention:-** Data loss prevention DLP technologies are those that prevent an organization employee from sharing valuable Company Information or sensitive data - whether unwittingly or with ill intent - outside the network

Email security:- Email Security is an ~~essp~~. especially important factor to consider when implementing network security tools.

Mobile device Security:- The vast majority of us have mobile device that Carry some form of personal or sensitive data we would like ~~of~~ to protected.

Firewall Security:

1. Firewall acts like a sentry for a Corporate network. Firewall stands b/w Corporate network and the outside world and prevent the network from outsider's attacks.

2. All the traffic b/w the network and the internet in either direction must pass through the firewall.

3. The firewall decides if the traffic can be allowed to flow or whether it must be stopped from proceeding further.

Section-3

Q.

Q-1

Approaches

In formation System resource are:

1. People : Enduser, IS Specialist
2. Hardware : Machine and media
3. Software : Program and procedures
4. Data : Data knowledge bank
5. Network : Communication media & network