**Precautionary measures taken by the system administrator(you) to secure the network:**

\* Ensure that you have across-the-board insight into your network environment, including memory usage, network traffic, CPU and capacity. Plus, analyze the databases to increase the security of the network meaning ease of access and control over the network system.

\*Remove the network shares which are redundant or unnecessary and put security in place for essential ones, such as printers to reduce the risk of malware which can easily spread across the network.

Always be aware while adding internet devices to your central network as this makes the system more susceptible to cyber attacks.

\*The network’s security settings are limited just to a particular network so, when our network devices connect to other networks, it’s possible that they adopt the other network’s security settings. As the external network’s security is beyond your control, it could potentially put the device at risk. To prevent this, you should restrict users from connecting devices to unapproved networks.

\*To reduce the risk of devices being fooled to connect to other network we should modify the current network’s default IP range. To enhance security even further, you should add firewall rules to ensure only approved users can connect.

\*To make sure any new software is compatible with the current system and network configuration, we should always test it on a virtual system first and then implement it on the actual system

\*Block unused IP ports by implementing firewall as an open port may enable malware like Trojan and worms which can hijack our network.

\* To protect the network from hacking or infection we need to have a complete overview of all the possible entry points into our system, including physical ones, such as pen drives. This involves access control, strengthening your firewall, removing physical ports ,etc.

\*Run critical systems on an isolated network to make sure that networking process is not halted even if there are some anomalies found on the system.