NIST Framework

Things that are essential:
1. Use **ANTI-VIRUS** and keep it up to date. Scan the system every day.

1. Identify

Try to understand the threat, or risk. what kind of risk it is? Or What causing the problem?

2. Protect

Save the system after identifying the issue or thereat. e.g. use of encryption, security, update system.

3. Detect

We need to monitor the system, that who or what is accessing. Investigate and check the network.

Report the attack, notify it to the stakeholder, Update the cybersecurity policy.

4. Respond

Repair and restore the system or network that were affected. Keep everyone informed about system respond or recovery update.

5. Recover