By taking example of WannaCry ransomware, which had occurred during 2017 has effected computer world in bad manner. By using this example, we relate the following terms:

- Threat: A threat is any potential danger that could exploit a vulnerability to breach security and cause possible harm. Here WannaCry ransomware was threat itself .It was designed to encrypt files on infected systems and demand a ransom for their decryption.

- Vulnerability: A vulnerability is a weakness or flaw in a system, network, or application that can be exploited by a threat. Here WannaCry exploited a specific **vulnerability** in Microsoft Windows operating systems known as **EternalBlue**. This vulnerability existed in the Server Message Block (SMB) protocol, which is used for file sharing between computers on a network.

- Attack: An attack is an attempt to exploit a vulnerability to cause damage, unauthorized access, or disruption to a system. The attack occurred when the WannaCry ransomware was unleashed across the globe, targeting systems with the EternalBlue vulnerability. Once the ransomware infected a system, it encrypted the user's files and displayed a ransom note demanding payment.

- Risk: Risk is the potential for loss or damage when a threat exploits a vulnerability. It is often quantified by the likelihood of an attack and the impact it could have. The **risk** involved in the WannaCry incident was the possibility of significant disruption and loss due to the encryption of critical files. Organizations faced risks such as operational downtime, loss of sensitive data, and financial losses.

- Exploit: An exploit is a piece of software, a set of commands, or a methodology that takes advantage of a vulnerability to carry out an attack. WannaCry used an **exploit** based on the EternalBlue vulnerability to spread itself. The exploit allowed the ransomware to move laterally across networks, infecting other vulnerable systems without human intervention.

- Asset: An asset is anything of value to an organization or individual that needs protection. This can include data, hardware, software, intellectual property, or even the reputation of an organization. The **assets** targeted by WannaCry were the files and data stored on the infected systems. These files were valuable to individuals and organizations, making them the primary focus of the ransomware's attack.

- Impact: Impact refers to the potential consequences or damage that could result from a successful attack or security breach. The **impact** of the WannaCry attack was substantial, affecting hundreds of thousands of computers in over 150 countries. The attack caused widespread disruption in various sectors, including healthcare, transportation, and manufacturing