Document on the term Threat, Vulnerability, Attack, Risk, Exploit, Asset, Impact choosing a well known cybersecurity incident Equifax data breach:

- **Threat:**

  A potential cause of an unwanted incident, which may result in harm to a system or organization. Examples include hackers, natural disasters, or insider threats.

  Threat regarding Equifax data breach:

  Sophisticated hackers or attackers seeking to obtain and steal private information presented a threat in the Equifax hack. These attackers were capable of taking advantage of holes in Equifax's systems and intended to do so.

  The threat actors probably targeted the massive amount of personal data that Equifax stored with the intention of stealing it for financial gain or identity theft. In the world of cyberspace, where attackers seek for valuable targets with potentially profitable data, this type of threat is frequent.

- **Vulnerability**:

  A weakness or flaw in a system or process that can be exploited by threats. For instance, outdated software or unpatched security holes can be vulnerabilities.

  Vulnerability regarding Equifax data breach:

  The open-source web application framework Apache Struts, which Equifax uses, has a known security vulnerability that was the basis of this case's vulnerability. Prior to the incident, a patch for this vulnerability was available and was described in a security bulletin.

  If left unpatched, a major vulnerability in Apache Struts might have enabled remote command execution on a server by attackers. Equifax's system was vulnerable to exploitation since they neglected to install the available security fixes.

- **Attack**:

  An intentional action taken to exploit a vulnerability in a system. This could be a cyber attack like phishing, a malware infection, or a physical break-in.

  Attack regarding Equifax data breach:

  To breach Equifax's network, the assault took advantage of an unpatched vulnerability in Apache Struts.

  The vulnerability was exploited by attackers to run commands on the web servers of Equifax. As soon as they had initial access, they could use the network to move around, increase their level of authority, and access databases that held private data. It is highly likely that the attackers employed sophisticated strategies to evade discovery and preserve entry.

- **Risk**:
  The potential for loss or damage when a threat exploits a vulnerability. It is typically assessed in terms of the likelihood of an attack and the impact it would have.

  Risk regarding Equifax data breach:

  The danger arose from the possible disclosure of private data, including residences, birth dates, and Social Security numbers.

  Due to the type and quantity of data involved, there was a very significant danger. The exposure of 147 million people's personal information raised serious concerns about fraud, identity theft, and other financial loss. Due to Equifax's tardiness in addressing the known issue, the danger was increased.

- **Exploit**:
  A method or piece of software that takes advantage of a vulnerability to perform an unauthorized action. For example, a hacker might use an exploit to gain unauthorized access to a network.

  Exploit regarding Equifax data breach:

  In this instance, the attack technique used by the attackers to leverage the Apache Struts vulnerability was known as the exploit.

  Hackers developed targeted payloads to take advantage of the unpatched vulnerability. This gave them access to sensitive data that they might potentially change or exfiltrate, as well as the ability to run unauthorized instructions on the server. Because the vulnerability was critical and well-documented but unpatched, the exploit was especially successful.

- **Asset**:
  Anything of value to an organization or individual that needs protection. Assets can be physical (like hardware), digital (like data), or intellectual (like patents).

  Asset regarding Equifax data breach:

  The sensitive personal information that Equifax had saved was the main asset in this hack.

  Social Security numbers, credit histories, and other private information belonging to millions of people were among Equifax's assets. Attackers are after this data because it may be used for financial crime and identity theft, making it valuable. Preserving these resources is essential to upholding confidence and averting damage.

- **Impact**:
  The consequence or effect of a successful attack or exploitation of a vulnerability. It describes the extent of damage or loss caused, such as financial loss, data breach, or reputational damage.

  <u>Impact regarding Equifax data breach:</u>

  One immediate consequence was the exposing of 147 million people's personal information, which raised the possibility of financial fraud and identity theft. Equifax suffered large financial losses as a result of the hack, including court settlements, fines from authorities, and expenses for security upgrades and cleanup. Additionally, it undermined customer confidence, tarnished Equifax's reputation, and brought lawmakers and regulators under more scrutiny. The hack brought attention to the need for improved cybersecurity procedures and changed how businesses approach vulnerability management and data security.