Some of the terms used in cyber security are:

**1. Threat:** A threat represents a potential risk that can exploit a weakness in a system. In the Equifax breach, the threat came from hackers aiming to access and misuse sensitive personal information for various malicious purposes.

**2. Vulnerability:** A vulnerability is a defect or gap in a system that can be exploited. For Equifax, the vulnerability was an outdated version of Apache Struts, which had not been updated with the necessary security patches, thereby exposing the system to unauthorized access.

**3. Attack:** An attack is the act of leveraging a vulnerability to inflict damage. In this case, attackers utilized the unpatched Apache Struts flaw to breach Equifax's network, siphon off confidential data, and transfer it outside the organization.

**4. Risk:** Risk is the potential for negative outcomes when a threat takes advantage of a vulnerability. The risk involved in the Equifax breach was the possible exposure of personal information of about 147 million individuals, which could result in identity theft, financial losses, and reputational harm to Equifax.

**5. Exploit:** An exploit is a method or technique used to leverage a vulnerability. In the Equifax incident, the exploit involved manipulating the unpatched flaw in Apache Struts to gain unauthorized control over Equifax’s servers and retrieve sensitive data.

**6. Asset:** An asset is a valuable component that needs safeguarding. For Equifax, the assets included the personal and financial data of their customers, such as Social Security numbers, dates of birth, addresses, and driver’s license information.

**7. Impact:** Impact refers to the effects or damage resulting from an attack. The Equifax breach led to significant consequences, including the theft of personal information of millions, extensive financial losses, severe damage to Equifax's reputation, and ongoing risks of identity theft for those affected.