Understanding Threats and Threat Actors

Let's start with the Risk.

Risk - Risk is the probability of a negative event to occur and its impact on something valuable.

It can be calculated with a simple formula. That is -

Risk = Likelihood × Impact

So, basically we can say that a risk associated with an asset derives from the likelihood of an event multiplied by the impact it cause.

Lets understand this with an example. Suppose we have a building as an asset and we want to calculate its risk. One risk to it can be fire. So we will take into consideration what is the likehood of an event that can cause fire in the building and after that we will look into the impact it will have.

We can deduce it with 4 quadrants

1. Low-probability, low impact events
2. Low-probability, high impact events
3. High-probability, low impact events
4. High-probability, high impact events

Moving on, we have threat.

What is a Threat ?

A threat is something that poses risk to an asset we care about protecting. In terms of cybersecurity, it could malware or virus.

Next, we have **Threat Actor**

Threat Actor is a person or group of people embodying a threat is known as a threat actor. Ex - Hackers.

Now, we have **Vulnerability and Exploit**.

So, A vulnerability is a flaw that allows a threat to cause harm. For example, a vulnerability in google chrome can get your hacked which will eventually cause you harm and your data.

Related to this, we have **exploit**

When a vulnerability in the system is used for unintended purposes by interacting with it then it is called Exploit.

At last, we have the **attack surface**.

It describes all the points of contact on our system or network that *could* be vulnerable to exploitation. For example, you own a business, the business has a office, it has its online website and social media channels. All the assets you have can come under an attack surface as they can be targeted by the attackers outside or inside your company.
