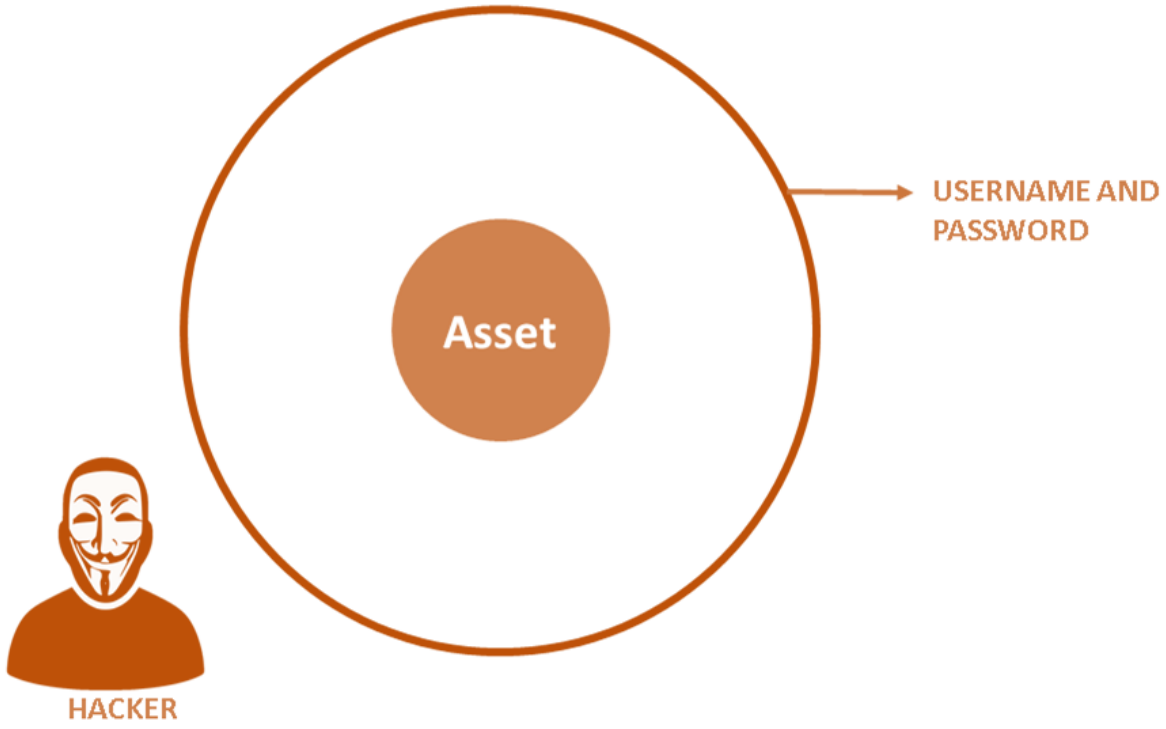
Cybersecurity Defense Models:

These models are mainly used for Defense Purpose such as securing the data or the asset. There are 2 main types of Cybersecurity Defense Models: Lollipop Model, and Onion Model. A multi-layered approach is set in place to reduce opportunities and access points for attackers. The idea is as simple as it sounds; instead of having only one layer of defense, you employ several layers, making it more difficult for cyber criminals to launch a successful attack.

1. Lollipop Model:

Lollipop Model is Defense Model associated with an analogy of a Lollipop. A lollipop is having a chocolate in the middle and around the chocolate, there is a layer of crust, mainly of sugar flavored syrup. A person licks and licks the lollipop and finally, the chocolate in the middle is exposed. Mapping this analogy of Lollipop to the Model, the hacker just needs to break that one layer of security to get hands on the asset, in this case, say it is Username and Password. Once it is done, the hacker can access the asset. So Lollipop Model is not a good model for Cybersecurity.



2. Onion Model:

Onion Model is Defense Model associated with an analogy of an Onion. An Onion is a vegetable which is composed of layers. Only by peeling each layer, we can get to the center of the Onion. Also, while peeling, we get tears in our eyes. Mapping this analogy of Onion to the Model, the hacker needs to break all the layers of security to get access to the asset. Breaking each layer such as Firewall, IDS/IPS, Authentication, Authorization, and Cryptography in this case, should bring tears to his eyes. In simple words, breaking each layer should be complex and extremely challenging for the hacker. So Onion Model is considered as a good model for Cybersecurity.

There are many layers and you have to peel each one and make sure there is proper security at every layer. When it comes to protecting a small business network from Ransomware, viruses, malware, improper browsing, etc., you have to have a layered approach to security.