**#1) Social Engineering Access:**

Situation – A mid-level user access account has been compromised as a result of social engineering, ie. gaining knowledge of there account credentials through personal information manipulation. This situation allows the attacker access to the system through valid means and may not be detected unless a password is changed or access is denied to the original user. Particular issues arise when the attacker goes on extended leave and cannot verify their access daily.

Extensions of this can be gaining of specific data without access, resulting damage to the company is confined to information leaked.

**#2) Web Application Access:**

Situation – Web/cloud/user application is compromised through some form of attached malware or improvised worm or trojan. Often detected by system anti-virus software or user permissions denied to install third party applications. Occurs mostly with systems with minimal firewall or antivirus software or libraries are not updated often.

**#3) Physical Penetration Access:**

Situation – Physical access is granted to a secured area that has access to information or systems of a sensitive nature. Often linked with social engineering or PSYOPS whereby human nature and interaction is leveraged to “guilt” a person into allowing access – often called tailgating. This can also include leaving workstations unlocked, doors or areas unsecured and un guarded for some period of time. Depending on the area accessed, the attacker can gain access to various levels of system integrity.

**#4) Network Services Access**:

Situation – Using normal access methods to a secured network by probing vulnerable software and/or hardware. Sometimes linked with web application access but stands alone as it mostly uses forced network access methods wih an attacker finding vulnerable access ports and packet manipulation in a common network architecture. Access is limited to the network breached but can expand further depending on the hardware that is able to be accessed.

**#6) Remote brute force access**:

Situation – Trying to log in to the systems connected through these modems by password guessing or brute-forcing. With advances in GPU and CPU technology, computers have higher potential to guess millions of passwords a second and can gain access through brute force activations. Similar damage and access to social engineering access as the system is not technically compromised (ie, the password is correct) and can go unnoticed unless users are vigilant and notice any systems changes. A form of attack that gains access but lays dormant until needed at a future time.

**#7) Wireless Security Access**:

Situation – Access to a network through Wireless network password guessing (brute force) or hardware system manipulation. Varying levels of attack and damage depending on the network connected to the wireless router. This attack requires physical proximity to the wireless network or router and can be easy to achieve if system passwords are not redefined from the factory settings.

All incidents will have some crossover in incident response requirements but should all have varying levels of data breach/detectivity. Some systems (wireless especially) are prone to ease of attacks if not hardened.