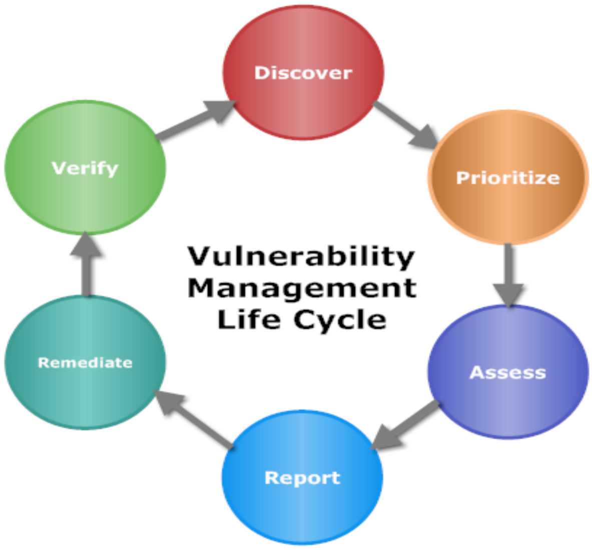
3. IoT vulnerability management



Another challenge is enterprise IoT is how quickly the patch for IoT device vulnerability can be made, how to prioritize the particular vulnerability.

Because most IoT devices require a firmware update in order to patch vulnerabilities, the task can be complex to accomplish on the fly. For example, if a printer requires firmware upgrading, IT departments are unlikely to be able to apply a patch as quickly as they would in a server or desktop system; upgrading custom firmware often requires extra time and effort.

Also the challenge for enterprises will be dealing with the default credentials which are provide to the user when IoT are first used. Oftentimes, devices such as wireless access points or printers come with known administrator IDs and passwords. On top of this, devices may provide a built-in Web server to which admins can remotely connect, log in and manage the device. This is a huge vulnerability that can put IoT devices into attackers' hands

. This requires enterprises to develop a stringent commissioning process. It also requires them to create a development environment where the initial configuration settings of the devices can be tested, scanned to identify any kind of vulnerabilities they present, validated and issues closed before the device is moved into the production environment.