In cybersecurity, an empiricist principle refers to the idea that security measures and strategies should be based on concrete evidence rather than on theories and assumptions. This means that decisions should be made by analyzing different threat patterns and behaviors to develop effective defenses. Two reasons why this principle is important in cybersecurity because it reduces reliance on theories and assumptions. By relying on accurate data, organizations can avoid using security measures that won't help against actual threats. Another reason is that it improves risk assessment. By analyzing historical date, it helps understand different cyber risks. On the other hand, the parsimony principle refers to using the simplest security solution to successfully asses a threat. This is also known as the Occam's Razor. One example of using the parsimony principle in cybersecurity is the password policy. Meaning that instead of creating a very complex password with special characters, a simpler way to make a password with a mix of upper/lowercase letters and numbers.