Journal Entry 2

1. Objectivity
    - Objectivity relates to cybersecurity in that we should be objective when developing it. For example, we should be objective when deciding sentencing times for cybercrimes.
2. Empiricism
    - When applying empiricism to cybersecurity, it means to look at things that are concrete. For example, cybersecurity analysts should be empirical when it comes to how much budget should go towards risk management, antivirus, etc. They shouldn't put most of their budget into risk management because they felt like it, but because they have studied that it is the most important component for the company to invest in.
3. Ethical Neutrality
    - We should take ethical neutrality into account in cybersecurity when it comes to data collection and usage. How much and what data should businesses be allowed to collect from customers? Should customers be alerted?
4. Parsimony
    - This principle is important when communicating with other branches of the company. The employees working outside of the IT security department are not going to understand certain terms and jargon related to cybersecurity. Therefore, instead of having to explain each term to them, the IT security department should put their thoughts into digestible wording.
5. Skepticism
    - Using skepticism in cybersecurity means to double check all possible vulnerabilities. Imagine if a company's systems had been breached, and some important data leaked. Then, let's say cybersecurity analyst find a vulnerability. Just because they found one vulnerability does not mean they found the cause of the leak. Using skepticism, they would have to rule out all other factors to make sure that vulnerability was the cause of the leak. This would include checking for any other vulnerabilities.
6. Determinism
    - In terms of cybersecurity, using determinism would mean that cyber crime analysts would have to find reason behind why cyber criminals partake in risky and illegal behavior. Is it for entertainment? Money? Something else? These are questions they would have to ask.
7. Relativism
    - Relativism in cybersecurity would be connecting other factors into technology and how it influences them. Not only considering the advancement of technology, but how it affects society, the economy, and policy.