Journal Entry 2

Question: Explain how the principles of science relate to cybersecurity ?

Before considering how the principles of science relate to cybersecurity one must consider that the principles can be applied to the study of cybersecurity through a social science framework. Understanding cybersecurity through a social science lens, requires us to recognize, how technological changes influences, the behavior dynamics, economic decision and policy making of the world. The way in which relativism relates to cybersecurity is that, it makes us recognize that changes in which occur in the fields , such as the healthcare systems, and critical in fracture systems, makes us aware, new technologies is always going to come with vulnerabilities, in which hackers can exploit, and that's where cybersecurity steps in. The way in which the principle of objectivity relates to cybersecurity, is that it gives cybersecurity professionals a unbiased opinion on addressing, security issues, that could tamper within a organization. This also helps them take an evidence-based approach, rather than who they feel is a suspect of a certain cybercrime, from the incident response report collected. The way in which the principle of parsimony relates to the field of cybersecurity, is that it makes data to understand in the field, very simple and not complex, for those with even no cybersecurity background able to learn. For example, if someone wanted to understand, how hackers can get into a system, using an attack method such as a phishing email, parsimony would be able to aid this issue, to make it as simple as possible to understand for people with no technological background. The way in which ethical neutrality, relates to cybersecurity, is that it is stating, that for law enforcement officials to look into a employee's life digitally or physically, they must adhere to protection rights, of the individual, to not break no laws, during their investigation, without a issued warrant to search.

The way in which determinism is related to cybersecurity, is that, it helps cyber professionals be able to determine how behavior is caused in cybersecurity, or how it influences preceding events in the future, when it comes to cybercrime.