Week 2 Journal Entry - Explain how the principles of science relate to cybersecurity.

Relativism- The theory of relativism states in basic terms that all things are related, this can be applied to cybersecurity in a chain of events perspective, this can start with the beginning of using passwords for security purposes, it was uncommon for people to use complex passwords and as such that led to people developing techniques to crack these simple passwords, as passwords became more complex, hackers continued to develop more sophisticated password crackers and hacking software to break into more complex networks.

Objectivity- The science of objectivity comes into play as researching must keep a level head when discussing controversial topics. Since the concept of objectivity states that science isn't to push a particular opinion and instead to increase the overall amount of knowledge, it is important that calculated decisions be made without personal opinions playing a factor.

Parsimony- The science of parsimony states that scientists should keep explanations as simple as possible, while it is often hard to keep answers related to cybersecurity in simple one or two sentence explanations, it is important that solutions don't become too overcomplicated.

Empiricism- Empiricism states that scientists should only study behaviors that appeal to the five senses, this can be applied to the field of cybersecurity, as it is irrational to collect information based off soft opinions instead of hard facts, as it can lead to compromised solutions.

Ethical neutrality- The concept of ethical neutrality states that scientists must apply to ethical standards regardless of the situation. Applying this to the concept of cybercrime, it is important to note that doing things such as denying access to the internet/computers for certain people or invading the privacy of potential cybercriminals are ethically wrong, although they could provide potential positive impacts.

The principle of determinism goes hand in hand with the issue of computer hacking in a similar fashion to relativism, as taking advantage of vulnerabilities are almost always a cause and effect scenario. For instance, the first cases of password cracking were resulting from people using weak passwords. Since computer hacking is defined in such a broad perspective, guessing a password on a computer is included. If computer passwords were complex from the start, people may have been more discouraged to attempt to develop machines that could help them guess passwords, since it wouldn't have been such common practice. Although it began with early simple password cracking techniques, these practices of hacking began to develop more and more over time and led to the more advanced technology that we have today.   Past successful attacks such as the Marriott hotels security breach were the result of previous actions. Marriott was the victim of a cyber attack because of the failure of the company to update its outdated and vulnerable network. This attack has also been suspected to possibly be part of a larger ploy by foreign countries to gain information on U.S. government officials that could have been staying at the hotel, further supporting the cause and effect nature of determinism.