Week 2 Journal Entry: Empiricism

How does the principle of empiricism enhance the effectiveness of cybersecurity practices? Reflect on how empirical data collection and analysis can help identify emerging threats, assess the effectiveness of current security measures, and guide the development of new strategies to protect information systems.

Empiricism is defined as the belief that social scientists can only study behavior which is real to the senses (what we can touch, see, taste, hear and smell). Using this definition, knowledge in our discipline must come from empirical research; we cannot rely on opinions or hunches as they would potentially lead to erroneous conclusions.

The way empiricism would enhance the effectiveness of cybersecurity practices is by having something tangible that you can test and analyze the results of. Without the ability to measure something with statistics and numbers, it is difficult to prove what works and what doesn't. In terms of cybersecurity, these would include things like the changes in attack methods (newer ones include SIM swapping and other means of social engineering), types of malware being used, which organizations are being targeted more often, and who compromises these cyber criminal enterprises.

Taking it one step further, when talking about specific incidents, both sides (white hat vs black hat hackers, red team vs blue team) need to rely on empirical data in order to execute their plans. When it comes to black hat hackers, they exploit vulnerabilities that have been proven to be exploitable. The opposite is also true - the white hat hackers use empirical data discovered by going over logs and monitoring networks. By figuring out patterns within the logs and traffic, they are able to better protect the organization from these attacks happening in the first place and also preparing for future incidents.

If the principle of empiricism was not used within the field of cybersecurity, there would be a lot more wasted time and effort spent on mitigating and/or resolving attacks. By using what has been proven to work and coming up with new methods, the cybersecurity team is able to pinpoint the problem easier and respond more rapidly.