CYSE 201S Journal Entry #2 Katherine Billy

How does the principle of empiricism enhance the effectiveness of cybersecurity practices?

The principle of empiricism enhances the effectiveness of cybersecurity practices by requiring the testing of everything. The principle of empiricism asks to check the facts and make sure that a system will work exactly how it is expected to, without relying on guesses. This includes investigating both systems that work and systems that don't in order to figure out the why and how.

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.

Cybersecurity and all its parts are continuously evolving and adapting, which is why theories and systems, both current and old, must continue to be tested and dissected in order to continue to learn and grow. Analyzing and examining the empirical data collected through the testing of cybersecurity systems is how new ways of protecting cyber systems are created and improved. By testing current security systems against the latest viruses and hacking techniques is how we learn what works and why it works.

References

Ali, A. (2025, April 29). *Cybersecurity Through an Empirical Lens: Leveraging Locke's Philosophy for Threat Intelligence*. Retrieved from Linkedin: https://www.linkedin.com/pulse/cybersecurity-through-empirical-lens-leveraging-lockes-ali-ali-l9w3f#:~:text=John%20Locke's%20empiricism%2C%20articulated%20in,compelling%20lens%20for%20understanding%20cybersecurity.

Page, D. (2023, February 20). *Cybersecurity Theory Review*. Retrieved from Linkedin: https://www.linkedin.com/pulse/cybersecurity-theory-review-zerotrustsolutions#:~:text=Evolutionary%20Theory%3A%20This%20theory%20argues,to%20the%20evolving%20threat%20landscape.