Gabrielle Gaston

CYSE 201: Week 2 Journal

The principles of science offer essential frameworks for addressing challenges and solving problems in cybersecurity. To begin, empiricism emphasizes the importance of data-driven decision-making, which is central to cybersecurity. Security teams rely on real-world data and observations, such as network traffic logs and intrusion detection alerts, to understand and address threats. Moreover, determinism suggests that certain outcomes reflect the predictable nature of events in cybersecurity. For instance, system breaches are often the result of predictable events such as misconfigurations or failed updates. By identifying these patterns, cybersecurity professionals can proactively prevent similar incidents. Additionally, Parsimony which is the principle of simplicity, aligns with the idea that effective security solutions are often the most simple, efficient solutions. The purpose is to align with the idea of minimizing security complexities to avoid overcomplicating defenses while still maintaining effectiveness. Overcomplicated security measures can create vulnerabilities; therefore, a balance between robustness and simplicity is crucial. Next, relativism in cybersecurity means recognizing that security practices must adapt based on different threat landscapes or organizational needs. These needs may vary depending on situations such as the specific threats, environment, or organizational goals. Additionally, objectivity is essential in cybersecurity to ensure decisions are made based on unbiased facts and evidence rather than assumptions or personal preferences, further supporting fair threat assessments and accurate responses. Equally important, skepticism drives cybersecurity experts to continuously test systems for weaknesses, identify vulnerabilities before they are exploited, question assumptions, and challenge the integrity of their defenses. Finally, ethical neutrality ensures that cybersecurity efforts focus on safeguarding data and systems without moral or political bias, ensuring fairness in protecting users and data privacy and security regardless of their background or affiliations across diverse environments.