Brendan Marcelo
CYSE201S
Journal Entry 2

Relativism looks at Cybersecurity in a systems perspective and suggests that changes in one's system leads to changes in another system. Changes in development of cyberspace, educational system, social systems, economics, criminal justice, and political systems shape how we approach and make changes to cybersecurity. Due to the growing reliance of technology in the school system whether it may be online class resources or programs required for teachers/professors, it raises awareness to the exposure of various vulnerabilities and calls for updated policies to ensure data of students and teachers are not compromised. The emergence of social media platforms are always growing and changing. Apps like Instagram, Facebook, X, etc., has introduced different behaviors that promote new ways to ensure that data is private, and the integrity of information is accurate. Economics is constantly emerging with e-commerce and different platforms for online banking, it raises awareness for continued updated protection against fraud and computer hacking.

Objectivity refers to the way scientists study topics in a value-free manner. This means studying cybersecurity without any bias, but rather on facts and evidence. Studies on how hackers should be punished should examine the magnitude of the event with supporting facts, data, and evidence, rather than promoting a particular viewpoint about the incident or the person engaging in these activities. When using technology to monitor sex offenders it requires analyzing data and effectiveness, rather than personal opinions on criminal justice. In cybersecurity, objectivism is essential because it promotes unbiased research.

Parsimony means that scientists should keep their levels of explanations as simple as possible. This is much more achievable in natural sciences than in social sciences. For instance, if one was to jump off a desk, why do they fall to the ground? In a natural science point of view, it is simply because of gravity. However, when it comes to the reasoning behind why people commit cybercrime, it is more complex due to the nature of human behavior. The "self-control theory" assumes that individuals commit crime because they have low self-control characterized by impulsivity and the feeling of immediate gratification. Parsimony is an efficient way to create a simple solution and theory to human's behavior in relation to cybersecurity vulnerabilities and threats.

Empiricism is defined as the study of behavior which is real to the senses such as touch, see, taste, hear or smell. Social scientists argue that we should not rely on opinions of hunches to frame our understanding of cybercrime. Through an empiricism lens, researchers studying hacker or cyber-criminal behavior must be based on accurate data, attack patterns, and penetration tests, rather than how or why the cybercrime occurred. This aspect of social science ensures that cybersecurity policies are based on facts and helps prevent inaccurate conclusions.

Ethical neutrality refers to the fact that scientists must adhere to ethical standards and avoiding biases when conducting research. It is essential to protect the rights of individuals objectively without ethical views interfering with the process. When monitoring students' online coursework, the ethical neutral approach is studying whether

monitoring enhances academic performance and honestly, rather than deciding if student monitoring is ethical or unethical. By remaining ethically neutral it ensures unbiased evidence-based results to cybersecurity challenges.

With that being said, the social science principles of relativism, parsimony, empiricism, and ethical neutrality ensures a poised solution to the study of cybersecurity challenges. Relativism focuses on how different systems influence cybersecurity on all platforms. Objectivity highlights unbiased solutions, while parsimony encourages simple solutions interconnected with human behavior in cybercrime. Empiricism underlines accurate data to create effective cybersecurity policies. Finally, ethical neutrality guarantees unbiased research and protects the rights of individuals. All of these social sciences offer a complete approach for understanding cybercrime in the world today.