Define each of the principals of science in your own words.Then, give an example of how each of the principals relates to cybersecurity.

Janae Craig

05/26/2024

Relativism in social science holds that truths and values are subjective and differ across cultures and individuals. It opposes universal norms and advocates for recognizing different viewpoints within their settings.Relativism emphasizes how it is linked to technology. This implies we must understand how technology influences behavior, legislation, and social dynamics. Understanding this allows us to better address cybersecurity concerns across several platforms.

Objectivity in social science strives for fairness and neutrality while minimizing biases. It uses empirical evidence and strict methodology to discover truths about human behavior. Researchers aim to maintain a neutral perspective. This is extremely important in cybersecurity research because it helps to minimize personal biases and researchers can ensure that their findings add to objective understanding rather than being influenced by subjective perspectives.

Choosing simple explanations over complex ones is known as parsimony in social science. By adopting straightforward theories with few assumptions, this aids researchers in conducting their work with greater clarity and fluency. In cybersecurity, network segmentation is one way to demonstrate parsimony. A parsimonious approach involves segmenting the network into smaller parts according to function or security rather than creating a single, massive network where all devices can communicate with ease. This simplification limits hackers and lowers the overall danger to the network, which in turn decreases the number of potential breaches and the intensity of cyberattacks.

Empiricism in social science is based on real-world data to better understand human behavior and society. Researchers collect data through methods such as polls, interviews, and studies to support or refute theoretical hypotheses. Relying entirely on real experiences and evidence ensures legitimate insights while avoiding subjective judgments or presumptions. This approach protects against incorrect outcomes, which improves the credibility and effectiveness of security measures.

Ethical neutrality in cybersecurity requires researchers to follow ethical principles. Social scientists investigating cybercrime encounter ethical issues such as data privacy and surveillance. Upholding ethics promotes responsible research and safeguards people's rights, resulting in the creation of ethical cybersecurity techniques.

Determinism claims that events follow predictable patterns based on these factors, which minimizes the significance of decision-making in shaping behavior and social change. Determinism in cybersecurity implies that online behaviors are influenced by previous events. Although some argue for free will, cyber-actions frequently follow predictable patterns based on previous events. Understanding determinism helps to anticipate and mitigate cyber threats, which improves overall cybersecurity measures.

References

Loiseau, Ventre, D., & Aden, H. (2020). *Cybersecurity in Humanities and Social Sciences [e-book] A Research Methods Approach.* John Wiley & Sons, Incorporated.

Findings from Singapore University of Social Sciences in Cybersecurity Reported. (2024). In *Journal of Engineering* (p. 759). NewsRX LLC.