JOURNAL ENTRY 2

Social Scientists are said to adhere to the principles of science as they study other topics and in conducting their research. These principles: relativism, objectivity, parsimony, empiricism, ethical neutrality, and determinism guides their methods and ensures the reliability of their findings.

Relativism

States that things are interrelated, they don't exist in isolation. Any given concept has no fixed level of importance but rather its status remains dependent on the setting in which it appears. However, for cybersecurity, it is a recognition that security practices and technologies need to be contextualised to the specific type of risk and threat, as well as the environment of an organization.

For example, a university and an e-commerce business both need to protect their digital assets. Belonging to different industries and they handle different types of data. Therefore, the security measures each may deploy will vary from the other.

Objectivity

Implies that one should think or make decisions using facts and information without being impersonal, being affected by emotions and should try to disregard personal biases. It is to maintain an impartial stance and pay attention only to facts to avoid letting judgements be based on unverified ideas and preconceived notions.

For example, when a credit card company's system is hacked, and their incident response team is called to conduct an investigation. In this case the team should be objective, instead of letting their personal biases affect their findings, they should focus on gathering factual evidence to understand the impact and identify the cause of the attack.

Parsimony

States that the simplest explanation is always the preferred one when it comes to any research data. It’s a way of ensuring scientific theories are as simple as possible and easy to understand, allowing new studies to be conducted from them.

For example, if a company wants to make the login access to their system more secure, this principle suggests adopting a simple and easy-to-use method instead of a complex multi-layered authentication system with multiple steps and hardware tokens. They should choose two-factor authentication: a password with a one-time code sent to a user’s phone. This strengthens security and can be easily understood and used by users.

Empiricism

Believes that knowledge is gained from careful observation and real-life experience. This principle stresses the importance of testing ideas practically to gather solid evidence. Similar to objectivity, it means research conclusions should not be influenced by personal opinion or emotion.

For example, a cybersecurity awareness program conducted for employees on risk management. Instead of thinking the employees will understand the training materials and implement the practices, the company applies the principle of empiricism by assessing the effectiveness of the program through observation and feedback. Conducts quizzes and surveys to gauge employees' understanding and through empirical observation tell the effectiveness of the program.

Ethical Neutrality

Means that when research is conducted, it should be done following ethical standards. It ensures the consideration of what is morally right or wrong and helps avoid biased assessments.

For example, a company contracted a Penetration Tester to assess their company's security posture. In simulating an attack to carry out vulnerability assessment it should be done without any conflict of interest. If vulnerabilities are found they shouldn't recommend solutions or vendors based on their personal preferences. In adhering to ethical neutrality, the penetration tester should ensure the assessment is free from external influence.

Determinism

This principle believes that a human's choice is influenced by previous events. In other words, occurrences can be predicted or the reasons behind them can be understood.

For example, an e-commerce business experiences a DDOS attack. Their incident response team conducts an investigation to find out how and why it happened. Upon completion they discover that staff clicked on malicious links in emails, which caused the system to be infected with malware. Understanding these past events helps predict and prevent future attacks.