Hans Peterson

CYSE 201S

1/10/2024

Journal Entry 2: Principles of Science

Objective: Explain how the principles of science relate to cybersecurity.

Objectivity guides policies and research in cybersecurity. Researchers diving into policies and laws, especially those regarding how technology should be used to monitor offenders, are areas where opinions and beliefs will clash, but objectivity presents a way to remove personal biases from the research. One example of biased research could be the interviewing subjects that all align with the researcher's beliefs. It may seem like a stretch, but I wonder if agencies like NIST can influence research results.

Parsimony keeps cybersecurity simple and easy to understand. For me, the CIA triad is memorable and recitable. Confidentiality, Integrity, and Availability. If a person knows the definition of those words and understands that the triad is within the context of information, they will understand what the CIA is about. Parsimony is crucial when it comes to clients who may not have any knowledge about cybersecurity. They are only as secure as they are knowledgeable about threats, social engineering, and other vulnerabilities that may exist in their companies. Many cyberattacks are the cause of human error.

I could apply empiricism to pen-testing and analysis in cybersecurity. Our presumptions of security cannot rely on belief; they need to be tested. Pen-testers and white-hat hackers exist for these purposes. On the criminal justice side of cybersecurity, empiricism would help with interviewing cybercriminals. It is important to know why they do it (Ex. profit, satisfaction), so a response can be made to inhibit or remove these reasons.

Ethical neutrality, like objectivity, guides policies, especially those of companies. I have received pop-ups asking for my consent on how my data will be handled by websites. It gives clients a level of transparency, increasing overall trust with the companies. Ethics is also important in the context of how much cybersecurity should be present. Would it be lax? Or would there be complete control over the systems? These policies could start infringing on comfort and, perhaps, rights.

Determinism explains the existence of cybersecurity. Since hackers and threats exist, cybersecurity exists to counteract them. It also explains hackers' behaviors. They will adapt to new systems and innovate new ways of bypassing security. This cycle repeats itself. The goal of cybersecurity is to break this cycle by patching out the vulnerabilities before hackers manage to exploit them.