Kerby Guillaume

As we know (or not know), there’s more to science than just a school course. Science can be dissected into various philosophies which may require more critical thinking to comprehend. With scientific thought, it is important to recognize the principles of science.

The principles of science are used as a knowledge base when it comes to scientific reasoning. First, we look at the principle of **empiricism** which is based on sole research. Introduced by Francis Bacon, empiricism completely shuts down the idea of opinion in science. The principle depends on strict evidence and believes in scientific research observation over opinions or assumptions. Philosopher Karl Popper introduces his theory of **post-positivism** which challenges the accuracy of scientific research. This principle states that science is almost never 100% and can possibly be proven wrong with the right evidence. Lastly, the principle of **natural philosophy** is probably the most common amongst researchers and is the basis of most theories. Known scientists like Sir Issac Newton and Galileo Galilei implemented this principle, stating that natural processes occur in a “cause and effect” system. Everything happens through natural processes.

**How do these principles relate to cybersecurity?**

**Empiricism.** Empiricism focuses on the data being shown. The principle shows that cybersecurity depends on output data because that is what we see. Therefore, cybercrimes must be proven through errors displayed in the system. If it cannot be proven, then we cannot base cybersecurity attacks on assumption.

**Post-Positivism.** This principle would require testing of data in order to ensure accuracy. Hypothesizes within cybersecurity must be able to be improved and updated so information in the systems are accurate and reliable.

**Natural Philosophy.** In relation to cybersecurity, this theory is equivalent to the analysis of the cause of attacks in cybersecurity. Reasoning using this principle focuses on the fact that cyber crimes happen for a reason and that it is important to decipher why these can happen. With this understanding, those working with the operating systems can take the necessary steps to avoid these attacks from continuing to happen.