There are several ways that the principles of science relate to and inform the field of cybersecurity:

Observation and data collection: Cybersecurity relies heavily on closely monitoring network traffic, devices, user behavior and more to gather intelligence about potential threats. This data is then analyzed using scientific methods.

Experimentation: Researchers conduct experiments, often in controlled labs, to better understand how vulnerabilities work and how to strengthen defenses. Trial-and-error helps advance theories.

Hypothesis development and testing: When unknown threats or issues emerge, analysts hypothesize possible explanations and test theories to determine root causes. This iterative process builds knowledge.

Classification and categorization: Just as scientists group living things, cyber incidents, malware strains, attack vectors etc. are systematically classified to facilitate analysis of patterns and relationships.

Evidence-based decision making: Recommendations for security improvements, tool/protocol development are founded on analyses of empirical data from past compromises rather than speculation alone.

Peer review: The security research community regularly shares and critiques findings to advance the body of scientific literature and identify flaws or missing angles before knowledge is applied.

Falsifiability: Claims about effective countermeasures or predictive models can and must be tested and possibly disproven, just as with scientific theories, to avoid misinformation.