Relativism means that security practices and views can differ depending on the culture, organization, or person. Because of this variety, objectivity is essential, which means analyzing security events, threats, and vulnerabilities based on facts and evidence, not personal opinions. Empiricism builds on this idea by stressing that we should always gather and study data to make decisions based on what we can measure and observe.

As we collect a lot of data, ethical neutrality becomes really important in security analysis. This means making sure our analysis stays objective and isn't swayed by personal beliefs while still considering the bigger ethical issues in security decisions. Basically, our conclusions and recommendations should be based on the facts, not on what we personally believe. Parsimony, or keeping things simple, helps us choose straightforward and efficient security solutions, which can reduce complexity and lower the chances of making mistakes or creating vulnerabilities.

Even with our best efforts, no security measure is perfect. This is why skepticism is essential—we must carefully assess new technologies, knowing they could bring new vulnerabilities. Skepticism should keep us cautious and alert, always looking for potential security risks. Finally, determinism connects all these ideas by saying that security incidents don't happen by chance; specific, identifiable factors cause them. By understanding these factors, we can better predict and prevent future threats, building confidence in our ability to create solid and effective security policies.