~~The article that I chose to review is "Improving vulnerability remediation through better~~ exploit prediction" from the Journal of Cybersecurity. With constant advancements being made within the technological and cybersecurity world, it is important to keep up with everything from the latest updates to newer cyberattacks. This article discusses how machine learning can help classify vulnerabilities from low to high risk for organization to help be better prepared to mitigate risks. The principles of social science include relativism, objectivity, parsimony, objectivity, skepticism, ethical neutrality, and determinism. The principal of relativism encourages us to explore change that has the potential to lead to major changes within cybersecurity. Empiricism is a principal that this research relates closely to this study because the sense that we can use for this study would be sight. We can physically see what the vulnerabilities are doing to the system, now we just have to figure out a cost-effective way to decrease the chance of high-risk attacks from happening. Determinism also relates because there is always a reason behind major vulnerabilities attacking systems with financial gain being a possible reason. The consequence of this actions can result in jail time for the attacker. This article relates closely to the principle of relativism because we are always looking for ways to improve processes within the cybersecurity realm due to new technology and vulnerabilities. The question that this study is challenging would be able to minimize the cost of protecting and managing assets and business systems. Organization are always at risk for major vulnerabilities to attack the system and to make processes more effective, organization risk from low to high would best help mitigate vulnerabilities within the system. To conduct this experiment data was collected from sources such as private data sets from partnered security firms and 75,000 vulnerabilities were documented. Rapid Automatic Keyword Extraction was also used to extract common words from each of the references in the CVE. There were also three key data sources

to include CVSS, published exploits, and reference tagging. This study relates to challenges faced by marginal groups because the research was done a financial standpoint and organization are always looking for ways to save money to protect company assets. The overall contributions that this research has done to society was that it helped organization and business find a more effective way to mitigate risks which has the potential to lead to major financial loss. Vulnerabilities can appear at any time and anywhere. The second contribution that this research has done for society would be helping businesses create policies on how to go about handling vulnerabilities which leads to a significance decrease in major incidents from taking place.

Jay Jacobs, Sasha Romanosky, Idris Adjerid, Wade Baker, Improving vulnerability remediation through better exploit prediction, *Journal of Cybersecurity*, Volume 6, Issue 1, 2020, tyaa015, https://doi.org/10.1093/cybsec/tyaa015